

BỘ TÀI CHÍNH

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập - Tự do - Hạnh phúc

Số: /2026/TT-BTC

Hà Nội, ngày tháng năm 2026

DỰ THẢO LẤY Ý KIẾN

...../...../2026

THÔNG TƯ

Quy định giao dịch điện tử trên thị trường chứng khoán

Căn cứ Luật Chứng khoán số 54/2019/QH14 được sửa đổi, bổ sung bởi Luật số 56/2024/QH15;

Căn cứ Luật Phòng, chống rửa tiền số 14/2022/QH15;

Căn cứ Luật Giao dịch điện tử số 20/2023/QH15;

Căn cứ Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15;

Căn cứ Luật An ninh mạng số 116/2025/QH15;

Căn cứ Luật Chuyển đổi số 148/2025/QH15;

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 19/2023/NĐ-CP ngày 28 tháng 4 năm 2023 của Chính phủ quy định chi tiết một số điều của Luật phòng, chống rửa tiền;

Căn cứ Nghị định số 165/2018/NĐ-CP ngày 24 tháng 12 năm 2018 của Chính phủ về giao dịch điện tử trong hoạt động tài chính;

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 được sửa đổi, bổ sung bởi Nghị định số 245/2025/NĐ-CP;

Căn cứ Nghị định số 69/2024/NĐ-CP ngày 25 tháng 6 năm 2024 của Chính phủ quy định về định danh và xác thực điện tử;

Căn cứ Nghị định số 137/2024/NĐ-CP ngày 23 tháng 10 năm 2024 của Chính phủ quy định về giao dịch điện tử của cơ quan nhà nước và hệ thống thông tin phục vụ giao dịch điện tử;

Căn cứ Nghị định số 165/2025/NĐ-CP ngày 30 tháng 6 năm 2025 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Dữ liệu;

Căn cứ Nghị định số 356/2025/NĐ-CP ngày 31 tháng 12 năm 2025 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân;

Căn cứ Nghị định số 29/2025/NĐ-CP ngày 24 tháng 02 năm 2025 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Tài chính được sửa đổi, bổ sung bởi Nghị định số 166/2025/NĐ-CP;

Theo đề nghị của Chủ tịch Ủy ban Chứng khoán Nhà nước;

Bộ trưởng Bộ Tài chính ban hành Thông tư quy định giao dịch điện tử trên thị trường chứng khoán.

Chương I

QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Thông tư này quy định về cung cấp dịch vụ trực tuyến trong hoạt động kinh doanh chứng khoán; hoạt động trao đổi thông tin điện tử trên thị trường chứng khoán; chế độ báo cáo, công bố thông tin về cung cấp dịch vụ trực tuyến và trách nhiệm của các cơ quan, tổ chức, cá nhân có liên quan.

Điều 2. Đối tượng áp dụng

Đối tượng áp dụng Thông tư này bao gồm:

1. Ủy ban Chứng khoán Nhà nước, Sở giao dịch chứng khoán Việt Nam và công ty con của Sở giao dịch chứng khoán Việt Nam (sau đây gọi là Sở giao dịch chứng khoán Việt Nam và công ty con), Tổng công ty lưu ký và bù trừ chứng khoán Việt Nam và công ty con của Tổng công ty lưu ký và bù trừ chứng khoán Việt Nam (sau đây gọi là Tổng công ty lưu ký và bù trừ chứng khoán Việt Nam và công ty con).

2. Tổ chức, cá nhân tham gia giao dịch điện tử trên thị trường chứng khoán bao gồm:

a) Tổ chức được phép hoạt động kinh doanh chứng khoán, lưu ký chứng khoán theo quy định của pháp luật về chứng khoán (sau đây gọi là tổ chức cung cấp dịch vụ) bao gồm: Công ty chứng khoán, công ty quản lý quỹ đầu tư chứng khoán; chi nhánh công ty chứng khoán, công ty quản lý quỹ nước ngoài tại Việt Nam; thành viên lưu ký; tổ chức được cấp Giấy chứng nhận đăng ký hoạt động phân phối chứng chỉ quỹ đại chúng;

b) Tổ chức, cá nhân sử dụng dịch vụ trực tuyến do tổ chức cung cấp dịch vụ cung cấp (sau đây gọi là khách hàng);

c) Các tổ chức, cá nhân khác có liên quan đến hoạt động giao dịch điện tử trên thị trường chứng khoán.

Điều 3. Giải thích từ ngữ

Trong Thông tư này, các từ ngữ dưới đây được hiểu như sau:

1. *Dịch vụ trực tuyến trong hoạt động kinh doanh chứng khoán* là dịch vụ kinh doanh chứng khoán được thực hiện bằng phương tiện điện tử do các tổ chức cung cấp dịch vụ cung cấp cho khách hàng trên môi trường mạng internet, mạng viễn thông, mạng máy tính khác (sau đây gọi là dịch vụ trực tuyến).
2. *Hệ thống giao dịch trực tuyến* là tập hợp các thiết bị phần cứng, phần mềm, cơ sở dữ liệu, hệ thống mạng viễn thông, mạng internet, mạng máy tính và các phương tiện điện tử khác để phục vụ quản lý và cung cấp dịch vụ trực tuyến trong hoạt động kinh doanh chứng khoán (sau đây gọi là hệ thống).
3. *Giao dịch chứng khoán trực tuyến* là các giao dịch liên quan đến chứng khoán được khách hàng thực hiện thông qua hệ thống giao dịch trực tuyến.
4. *Dịch vụ giao dịch chứng khoán trực tuyến* là các dịch vụ trực tuyến cung cấp cho khách hàng để mở tài khoản giao dịch chứng khoán và thực hiện giao dịch chứng khoán trực tuyến.
5. *Phần mềm ứng dụng trực tuyến* là phần mềm ứng dụng cung cấp dịch vụ trực tuyến trong hoạt động kinh doanh chứng khoán.
6. *Phần mềm ứng dụng Mobile App* là phần mềm ứng dụng trực tuyến được cài đặt trên thiết bị di động.
7. *Chứng từ điện tử trong lĩnh vực chứng khoán* là thông điệp dữ liệu về hoạt động giao dịch điện tử trên thị trường chứng khoán được tạo ra, được gửi, được nhận, được lưu trữ bằng phương tiện điện tử.
8. *Thông tin định danh thiết bị* là thông tin gắn với mỗi thiết bị dùng để nhận dạng thiết bị khi thực hiện dịch vụ trực tuyến.
9. *Sự cố nghiêm trọng* là các sự cố kỹ thuật xảy ra đối với hệ thống giao dịch trực tuyến hoặc hệ thống giao dịch chứng khoán giữa Sở giao dịch chứng khoán Việt Nam và công ty con với thành viên hoặc cổng giao tiếp trực tuyến, cổng giao tiếp điện tử cho các hoạt động nghiệp vụ của Tổng công ty lưu ký và bù trừ chứng khoán Việt Nam và công ty con với thành viên, gây hậu quả làm hệ thống giao dịch trực tuyến hoặc hệ thống giao dịch chứng khoán hoặc cổng giao tiếp phải dừng hoặc tạm dừng hoạt động hoặc bị chiếm quyền điều khiển, bị xâm nhập trái phép, bị đánh cắp, bị rò rỉ dữ liệu.
10. *Giao diện lập trình ứng dụng (Application Programming Interface - API)* là giao diện cho phép giao tiếp giữa các ứng dụng phần mềm trong tổ chức

cung cấp dịch vụ hoặc giữa tổ chức cung cấp dịch vụ với bên thứ ba theo phạm vi, điều kiện được kiểm soát.

11. *Bên thứ ba* là tổ chức có hợp đồng, thỏa thuận với tổ chức cung cấp dịch vụ về sử dụng API để cung cấp dịch vụ cho khách hàng.

12. *Thông tin sinh trắc học* là những dữ liệu về thuộc tính vật lý, đặc điểm sinh học cá biệt và ổn định của một người để nhận diện, phân biệt người này với người khác bao gồm: ảnh khuôn mặt, vân tay, móng mắt, ADN, giọng nói.

13. *Xác thực khớp đúng thông tin sinh trắc học* là việc đối chiếu, so sánh để bảo đảm trùng khớp thông tin sinh trắc học của khách hàng đang thực hiện giao dịch với thông tin sinh trắc học của khách hàng đã được thu thập, lưu trữ theo quy định tại Thông tư này.

14. *Xác thực khớp đúng thông tin sinh trắc học thiết bị* là việc đối chiếu, so sánh để bảo đảm trùng khớp thông tin sinh trắc học của khách hàng đang thực hiện giao dịch với thông tin sinh trắc học của khách hàng đã lưu trữ trên thiết bị di động của khách hàng.

15. *Xác thực yếu tố bí mật* là hình thức xác thực bằng các thông tin bí mật chỉ cá nhân khách hàng biết, bao gồm mã khóa bí mật (Password), mã PIN (Personal Identification Number), câu hỏi bí mật hoặc các thông tin bí mật khác do khách hàng đăng ký với tổ chức cung cấp dịch vụ.

16. *Phiên đăng nhập* là phiên khách hàng đăng nhập hệ thống giao dịch trực tuyến để thực hiện các giao dịch chứng khoán trực tuyến.

17. *Đặt lệnh qua điện thoại* là phương thức đặt lệnh mà khách hàng sử dụng số điện thoại đã đăng ký để gọi điện qua mạng di động đến tổ chức cung cấp dịch vụ, yêu cầu nhân viên môi giới đặt lệnh giao dịch chứng khoán.

18. *Xác thực bằng mã khóa bí mật dùng một lần (One Time Password - OTP)* là hình thức khách hàng xác thực giao dịch bằng mã khóa bí mật trong đó mã khóa bí mật do hệ thống gửi đến có giá trị sử dụng một lần và có hiệu lực trong một khoảng thời gian nhất định.

19. *SMS OTP* là hình thức khách hàng xác thực giao dịch thông qua mã OTP được hệ thống gửi qua tin nhắn SMS (Short Message Services) hoặc tin nhắn thông qua dịch vụ viễn thông cơ bản trên Internet.

20. *Voice OTP* là hình thức khách hàng xác thực thông qua mã OTP được hệ thống gửi qua cuộc gọi thoại hoặc cuộc gọi thông qua dịch vụ viễn thông cơ bản trên Internet.

21. *Email OTP* là hình thức khách hàng xác thực thông qua mã OTP được hệ thống gửi qua thư điện tử.

22. *Thẻ ma trận OTP* là hình thức khách hàng xác thực thông qua mã OTP được xác định từ một bảng 2 chiều (dòng, cột), tương ứng với mỗi dòng, cột là một mã OTP.

23. *Soft OTP* là hình thức xác thực thông qua mã OTP được tạo bởi phần mềm cài đặt trên thiết bị di động của khách hàng, phần mềm Soft OTP có thể là phần mềm độc lập hoặc được tích hợp với phần mềm ứng dụng chứng khoán trực tuyến.

24. *Token OTP* là hình thức xác thực thông qua mã OTP tạo bởi thiết bị chuyên dụng.

25. *FIDO (Fast IDentity Online)* là hình thức xác thực giao dịch sử dụng thuật toán khóa không đối xứng, bao gồm khóa bí mật được lưu giữ an toàn trên thiết bị của khách hàng dùng để ký số và khóa công khai dùng để kiểm tra chữ ký số.

26. *Xác thực hai kênh* là hình thức xác thực khi khách hàng thực hiện giao dịch, hệ thống giao dịch sẽ gửi thông tin yêu cầu xác thực giao dịch đến thiết bị di động của khách hàng qua cuộc gọi thoại hoặc cuộc gọi thông qua dịch vụ viễn thông cơ bản trên internet hoặc qua mã tin nhắn nhanh USSD (Unstructured Supplementary Service Data) hoặc qua phần mềm chuyên dụng, khách hàng phản hồi trực tiếp qua kênh đã kết nối để xác thực hoặc không xác thực thực hiện giao dịch.

27. *Đơn vị có thẩm quyền kiểm tra, đánh giá an ninh mạng* là tổ chức chuyên môn được cơ quan có thẩm quyền cấp phép; tổ chức sự nghiệp nhà nước có chức năng, nhiệm vụ phù hợp hoặc tổ chức chuyên môn được cấp có thẩm quyền chỉ định thực hiện.

Điều 4. Nguyên tắc giao dịch điện tử trên thị trường chứng khoán

1. Giao dịch điện tử trên thị trường chứng khoán phải bảo đảm nguyên tắc chính xác, công bằng, công khai, minh bạch, an toàn, bảo mật, hiệu quả và phù hợp với Luật Chứng khoán, Luật Giao dịch điện tử, Luật An ninh mạng, Luật khác có liên quan và các văn bản quy định chi tiết, hướng dẫn thi hành các Luật này.

2. Bảo đảm tính bí mật, tính toàn vẹn của thông tin khách hàng; bảo đảm tính sẵn sàng của hệ thống để cung cấp dịch vụ một cách liên tục.

3. Hệ thống chỉ được hoạt động cung cấp dịch vụ cho khách hàng khi bảo đảm an toàn, bảo mật theo quy định của Thông tư này và các quy định của pháp luật liên quan.

Chương II

CUNG CẤP DỊCH VỤ TRỰC TUYẾN TRONG HOẠT ĐỘNG KINH DOANH CHỨNG KHOÁN

Mục 1

QUY ĐỊNH CHUNG VỀ CUNG CẤP DỊCH VỤ TRỰC TUYẾN TRONG HOẠT ĐỘNG KINH DOANH CHỨNG KHOÁN

Điều 5. Yêu cầu chung đối với tổ chức cung cấp dịch vụ

1. Tổ chức cung cấp dịch vụ phải công bố thông tin về các dịch vụ cung cấp, bảo đảm khách hàng có khả năng tiếp cận được thông tin trước hoặc ngay tại thời điểm đăng ký sử dụng dịch vụ.

2. Nội dung thông tin công bố bao gồm:

a) Cách thức cung cấp dịch vụ, cách thức truy cập dịch vụ tương ứng với từng phương tiện truy cập;

b) Hạn mức giao dịch (nếu có) và các hình thức xác thực giao dịch;

c) Các trang thiết bị cần thiết để sử dụng dịch vụ, điều kiện để sử dụng các trang thiết bị;

d) Các rủi ro liên quan đến việc sử dụng dịch vụ trực tuyến theo quy định tại khoản 1 Điều 26 Thông tư này;

đ) Các thông tin khác về dịch vụ mà tổ chức cung cấp dịch vụ thấy cần thiết phải công bố.

3. Công ty chứng khoán phải được Ủy ban Chứng khoán Nhà nước chấp thuận trước khi cung cấp dịch vụ giao dịch chứng khoán trực tuyến. Hồ sơ đăng ký chấp thuận theo quy định tại Điều 203 Nghị định 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. Tài liệu về nhân sự vận hành hệ thống, hệ thống giao dịch, giải pháp kỹ thuật bảo đảm an toàn hệ thống, hệ thống lưu trữ dữ liệu dự phòng và khắc phục sự cố thực hiện theo mẫu quy định tại Phụ lục I ban hành kèm theo Thông tư này.

4. Việc cung cấp dịch vụ trực tuyến với khách hàng phải được thể hiện bằng hợp đồng hoặc điều khoản của hợp đồng, trong đó bao gồm các thông tin sau:

a) Phương thức giao dịch trực tuyến, loại giao dịch tương ứng với từng phương thức giao dịch;

b) Số điện thoại di động đăng ký sử dụng dịch vụ của khách hàng. Tổ chức cung cấp dịch vụ có biện pháp xác minh để bảo đảm số điện thoại này thuộc quyền sử dụng hợp pháp của khách hàng.

c) Các rủi ro có thể xảy ra khi thực hiện giao dịch trực tuyến theo quy định tại điểm d khoản 1 Điều này; trách nhiệm bồi thường của mỗi bên khi xảy ra rủi ro và trách nhiệm khác liên quan đến hoạt động giao dịch trực tuyến.

5. Tổ chức cung cấp dịch vụ có trách nhiệm ban hành quy trình giao dịch trực tuyến phù hợp với quy định của Thông tư này, quy định của pháp luật về chứng khoán và các quy định của pháp luật có liên quan.

6. Ghi nhận thông tin về các yêu cầu giao dịch của khách hàng trên hệ thống giao dịch trực tuyến. Các thông tin này phải lưu trữ để tra cứu được khi cần thiết.

7. Thông báo kết quả thực hiện lệnh giao dịch cho khách hàng ngay sau khi lệnh được khớp trên hệ thống giao dịch trực tuyến, bảo đảm không vượt quá 10 giây kể từ thời điểm lệnh được khớp.

8. Khi cung cấp dịch vụ cho khách hàng, công ty chứng khoán phải trực tiếp thực hiện các công việc sau:

a) Xác thực giao dịch mở tài khoản chứng khoán;

b) Xác thực giao dịch đặt lệnh mua bán chứng khoán;

c) Kiểm soát tính hợp lệ của lệnh đặt và chuyển lệnh vào hệ thống giao dịch chứng khoán của Sở giao dịch chứng khoán Việt Nam và công ty con.

9. Trường hợp kết nối hệ thống với bên thứ ba thông qua API để cung cấp dịch vụ, tổ chức cung cấp dịch vụ phải bảo đảm tuân thủ quy định tại khoản 8 Điều này, Điều 14, Điều 15 và Điều 22 của Thông tư này.

Điều 6. Yêu cầu đối với cung cấp dịch vụ trực tuyến của Sở giao dịch chứng khoán Việt Nam và công ty con, Tổng công ty lưu ký và bù trừ chứng khoán Việt Nam và công ty con

1. Bảo đảm việc cung cấp dịch vụ trực tuyến cho thành viên được thực hiện theo nguyên tắc công khai, công bằng, minh bạch, an toàn và hiệu quả; áp dụng thống nhất đối với mọi thành viên sử dụng cùng một loại dịch vụ.

2. Việc xây dựng hệ thống kết nối đến thành viên phải tuân thủ các quy định của pháp luật về bảo vệ an ninh mạng đối với hệ thống thông tin theo cấp độ đã được phê duyệt.

Điều 7. Các hình thức xác thực giao dịch điện tử

1. Xác thực bằng mã khóa bí mật dùng một lần (One Time Password - OTP).
2. Xác thực khớp đúng thông tin sinh trắc học.
3. Xác thực khớp đúng thông tin sinh trắc học thiết bị.
4. Xác thực Fast IDentity Online - FIDO.
5. Xác thực hai kênh: Yêu cầu xác thực của hình thức xác thực hai kênh có hiệu lực tối đa trong vòng 05 phút kể từ thời điểm hệ thống tạo yêu cầu xác thực.
6. Xác thực sử dụng chữ ký số.

Điều 8. Xác thực bằng mã khóa dùng một lần (OTP)

1. SMS OTP phải đáp ứng các yêu cầu sau:
 - a) OTP gửi tới khách hàng phải kèm thông tin thông báo để khách hàng nhận biết được mục đích của OTP;
 - b) OTP có hiệu lực tối đa 05 phút kể từ thời điểm được hệ thống tạo.
2. Voice OTP phải đáp ứng các yêu cầu sau:
 - a) OTP gửi tới khách hàng phải kèm thông tin thông báo để khách hàng nhận biết được mục đích của OTP;
 - b) OTP có hiệu lực tối đa 03 phút kể từ thời điểm cuộc gọi được hệ thống thiết lập thành công.
3. Email OTP phải đáp ứng các yêu cầu sau:
 - a) OTP gửi tới khách hàng phải kèm thông tin thông báo để khách hàng nhận biết được mục đích của OTP;
 - b) OTP có hiệu lực tối đa 05 phút kể từ thời điểm được hệ thống tạo.
4. Thẻ ma trận OTP phải đáp ứng các yêu cầu sau:
 - a) Thẻ ma trận OTP có thời hạn sử dụng tối đa 01 năm kể từ ngày đăng ký thẻ;
 - b) Yêu cầu xác thực OTP có hiệu lực tối đa 02 phút kể từ thời điểm được hệ thống tạo.
5. Soft OTP phải đáp ứng các yêu cầu sau:
 - a) Trường hợp phần mềm Soft OTP độc lập với phần mềm ứng dụng Mobile App, phải được tổ chức cung cấp dịch vụ đăng ký, quản lý phần mềm tại

kho ứng dụng chính thức của hãng cung cấp hệ điều hành cho thiết bị di động và hướng dẫn cài đặt trên trang thông tin điện tử của tổ chức cung cấp dịch vụ;

b) Phần mềm phải có chức năng xác thực khách hàng khi sử dụng lần đầu hoặc khi sử dụng trên thiết bị khác với thiết bị sử dụng lần gần nhất. Việc xác thực khách hàng phải bảo đảm khớp đúng SMS OTP hoặc Voice OTP thông qua số điện thoại di động đã được khách hàng đăng ký với tổ chức cung cấp dịch vụ và khớp đúng thông tin sinh trắc học của khách hàng theo một trong các loại thông tin sinh trắc học quy định tại khoản 12 Điều 3 Thông tư này;

c) Phần mềm Soft OTP phải yêu cầu kích hoạt trước khi sử dụng. Mã kích hoạt sử dụng Soft OTP do tổ chức cung cấp dịch vụ cung cấp cho khách hàng và chỉ được sử dụng để kích hoạt trên một thiết bị di động. Mã kích hoạt phải được thiết lập thời hạn hiệu lực sử dụng;

d) Phần mềm Soft OTP phải có chức năng kiểm soát truy cập. Trường hợp truy cập sai liên tiếp quá số lần do tổ chức cung cấp dịch vụ quy định (nhưng không quá 10 lần), phần mềm Soft OTP phải tự động khóa không cho khách hàng sử dụng tiếp. Tổ chức cung cấp dịch vụ chỉ mở khóa phần mềm Soft OTP khi khách hàng yêu cầu và phải kiểm tra, nhận biết khách hàng trước khi thực hiện mở khóa, bảo đảm chống gian lận, giả mạo;

đ) Mã OTP có hiệu lực tối đa 02 phút kể từ thời điểm được hệ thống tạo.

6. Token OTP: OTP có hiệu lực tối đa 02 phút kể từ thời điểm được hệ thống tạo.

Điều 9. Xác thực khớp đúng thông tin sinh trắc học

1. Việc áp dụng hình thức khớp đúng thông tin sinh trắc học sử dụng khuôn mặt phải bảo đảm:

a) Có độ chính xác được xác định theo tiêu chuẩn quốc tế như sau (hoặc tương đương): Có tỷ lệ từ chối sai $< 5\%$ với tỷ lệ chấp nhận sai $< 0,01\%$ theo tiêu chuẩn FIDO Biometric Requirement (áp dụng đối với tập mẫu tối thiểu 10.000 mẫu);

b) Có khả năng phát hiện tấn công giả mạo thông tin sinh trắc học của vật thể sống (Presentation Attack Detection - PAD) theo tiêu chuẩn FIDO Biometric Requirement (hoặc tương đương) để phòng, chống gian lận, giả mạo khách hàng qua hình ảnh, video, mặt nạ 3D.

2. Trường hợp áp dụng các hình thức khớp đúng thông tin sinh trắc học khác phải bảo đảm khả năng phát hiện, ngăn chặn hành vi gian lận, giả mạo khách hàng theo tiêu chuẩn tương đương quy định tại khoản 1 Điều này.

3. Giải pháp phát hiện tấn công giả mạo thông tin sinh trắc học của vật thể sống (Presentation Attack Detection - PAD) theo quy định tại điểm b khoản 1 Điều này do tổ chức cung cấp dịch vụ tự triển khai hoặc sử dụng của bên thứ ba phải được cấp chứng nhận bởi Liên minh FIDO (FIDO Alliance) hoặc tổ chức quốc tế khác có tiêu chuẩn đánh giá tương đương hoặc cao hơn.

4. Trường hợp khách hàng xác thực bằng hình thức khớp đúng thông tin sinh trắc học quá số lần sai liên tiếp do tổ chức cung cấp dịch vụ quy định (nhưng không quá 10 lần): hệ thống khóa chức năng thực hiện xác thực giao dịch bằng hình thức khớp đúng thông tin sinh trắc học, chỉ mở khóa khi khách hàng yêu cầu và phải kiểm tra, nhận biết khách hàng trước khi thực hiện, bảo đảm chống gian lận, giả mạo.

5. Thời gian thực hiện khớp đúng thông tin sinh trắc học tối đa 03 phút kể từ thời điểm hệ thống ghi nhận yêu cầu xác thực của khách hàng.

6. Tổ chức cung cấp dịch vụ phải đối chiếu khớp đúng thông tin sinh trắc học của khách hàng với một trong các dữ liệu sau:

a) Dữ liệu sinh trắc học được lưu trong bộ phận lưu trữ thông tin được mã hóa của thẻ căn cước công dân hoặc thẻ căn cước đã được xác thực chính xác là do cơ quan Công an cấp hoặc thông qua xác thực tài khoản định danh điện tử của người đó do Hệ thống định danh và xác thực điện tử tạo lập;

b) Dữ liệu sinh trắc học đã được thu thập và kiểm tra; bảo đảm sự khớp đúng giữa dữ liệu sinh trắc học của người đó với dữ liệu sinh trắc học trong bộ phận lưu trữ thông tin được mã hóa của thẻ căn cước công dân hoặc thẻ căn cước đã được xác thực chính xác là do cơ quan Công an cấp, hoặc với dữ liệu sinh trắc học của người đó thông qua xác thực tài khoản định danh điện tử do Hệ thống định danh và xác thực điện tử tạo lập;

c) Dữ liệu sinh trắc học của người đó được lưu trong Cơ sở dữ liệu quốc gia về dân cư trong trường hợp sử dụng thẻ căn cước công dân không có bộ phận lưu trữ thông tin được mã hóa.

Điều 10. Xác thực khớp đúng thông tin sinh trắc học thiết bị

Xác thực khớp đúng thông tin sinh trắc học thiết bị phải đáp ứng các yêu cầu sau:

1. Chỉ cho phép kích hoạt sử dụng sau khi có sự đồng ý của khách hàng và khách hàng đã thực hiện ít nhất một giao dịch thành công bằng hình thức xác thực khác.

2. Thời gian thực hiện khớp đúng thông tin sinh trắc học tối đa 02 phút kể từ thời điểm thiết bị bắt đầu thực hiện việc xác thực.

Điều 11. Xác thực Fast IDentity Online - FIDO

Xác thực FIDO phải đáp ứng các yêu cầu sau:

1. Khóa bí mật được lưu giữ an toàn trên thiết bị của khách hàng. Khách hàng sử dụng hình thức xác thực bằng mã PIN hoặc khớp đúng thông tin sinh trắc học thiết bị để truy cập, sử dụng khóa bí mật khi thực hiện giao dịch.
2. Khóa công khai được lưu trữ an toàn tại tổ chức cung cấp dịch vụ và được liên kết với tài khoản giao dịch trực tuyến của khách hàng.
3. Giải pháp do tổ chức cung cấp dịch vụ tự triển khai hoặc sử dụng của bên thứ ba cung cấp phải được cấp chứng nhận của tổ chức được Liên minh FIDO (FIDO Alliance) công nhận.

Điều 12. Áp dụng hình thức xác thực giao dịch điện tử

1. Việc mở, đóng tài khoản giao dịch chứng khoán, tài khoản lưu ký chứng khoán bằng phương tiện điện tử được xác thực như sau:
 - a) Áp dụng hình thức xác thực theo quy định tại Điều 9 Thông tư này đối với khách hàng là cá nhân và người đại diện hợp pháp đối với khách hàng là tổ chức;
 - b) Hợp đồng giữa tổ chức cung cấp dịch vụ và khách hàng phải được hai bên xác nhận bằng chữ ký số.
2. Các giao dịch chứng khoán trực tuyến được xác thực như sau:
 - a) Áp dụng hình thức xác thực theo quy định tại Điều 9 Thông tư này đối với khách hàng là cá nhân và người đại diện hợp pháp đối với khách hàng là tổ chức;
 - b) Việc xác thực giao dịch phải được thực hiện ít nhất đối với giao dịch đầu tiên của mỗi phiên đăng nhập của khách hàng;
 - c) Tổ chức cung cấp dịch vụ phải có biện pháp kỹ thuật để bảo đảm việc xác thực giao dịch và giao dịch của khách hàng được thực hiện trên cùng một thiết bị.
3. Trường hợp đặt lệnh qua điện thoại, khách hàng sử dụng số điện thoại đã đăng ký và cung cấp tối thiểu thông tin gồm: số định danh cá nhân, thông tin xác thực yếu tố bí mật. Giao dịch chỉ được thực hiện khi thông tin khách hàng cung cấp trùng khớp với thông tin khách hàng đã đăng ký và lưu trong hệ thống giao dịch trực tuyến.
4. Các giao dịch rút, chuyển tiền ra khỏi tài khoản giao dịch chứng khoán được xác thực như sau:

a) Với giá trị giao dịch dưới mười (10) triệu VND: áp dụng tối thiểu một trong các hình thức xác thực theo quy định tại Điều 7 Thông tư này;

b) Với số tiền giao dịch bằng hoặc trên mười (10) triệu VND: áp dụng tối thiểu hình thức xác thực theo quy định tại Điều 9 Thông tư này.

5. Đối với các giao dịch không thuộc các trường hợp quy định tại khoản 1, 2, 3, 4 Điều này, tổ chức cung cấp dịch vụ phân loại và đánh giá mức độ rủi ro để thỏa thuận với khách hàng về hình thức xác thực giao dịch phù hợp, áp dụng theo một trong các hình thức quy định tại Điều 7 Thông tư này.

Điều 13. Mở, sử dụng và đóng tài khoản giao dịch chứng khoán, tài khoản lưu ký chứng khoán của nhà đầu tư nước ngoài

1. Nhà đầu tư nước ngoài cư trú tại Việt Nam khi mở, sử dụng, đóng tài khoản giao dịch chứng khoán, tài khoản lưu ký chứng khoán bằng phương tiện điện tử thực hiện theo quy định tại Điều 12 Thông tư này.

2. Nhà đầu tư nước ngoài không cư trú tại Việt Nam thực hiện hoạt động đầu tư gián tiếp tại Việt Nam được ủy quyền cho tổ chức kinh doanh chứng khoán nước ngoài đại diện hoặc tổ chức có hợp đồng dịch vụ với nhà đầu tư nước ngoài để mở, sử dụng và đóng tài khoản giao dịch chứng khoán, tài khoản lưu ký chứng khoán bằng phương tiện điện tử tại tổ chức cung cấp dịch vụ. Tổ chức cung cấp dịch vụ phải thực hiện nhận biết đối với nhà đầu tư nước ngoài và tổ chức được ủy quyền theo quy định pháp luật về phòng, chống rửa tiền.

3. Việc mở, sử dụng và đóng tài khoản giao dịch chứng khoán, tài khoản lưu ký chứng khoán bằng phương tiện điện tử để thực hiện hoạt động đầu tư gián tiếp tại Việt Nam của nhà đầu tư nước ngoài không cư trú tại Việt Nam thực hiện như sau:

a) Không áp dụng quy định tại điểm a, b khoản 8 Điều 5; Điều 9; điểm b khoản 1 Điều 12; khoản 4 Điều 12 Thông tư này;

b) Tổ chức cung cấp dịch vụ có biện pháp kỹ thuật sử dụng hình thức xác nhận bằng phương tiện điện tử để thể hiện sự chấp thuận của nhà đầu tư nước ngoài hoặc tổ chức được ủy quyền đối với các nội dung mở, sử dụng và đóng tài khoản giao dịch chứng khoán, tài khoản lưu ký chứng khoán;

c) Tổ chức cung cấp dịch vụ có giải pháp kỹ thuật để thực hiện kiểm tra tính hợp pháp, hợp lệ và đối chiếu bảo đảm sự khớp đúng, chính xác của các tài liệu, thông tin, dữ liệu điện tử mà khách hàng cung cấp và tiến hành xác minh thông tin nhận biết khách hàng theo quy định pháp luật về phòng, chống rửa tiền;

d) Tuân thủ các quy định của pháp luật về chứng khoán có liên quan đến mở, sử dụng, đóng tài khoản chứng khoán, tài khoản lưu ký chứng khoán.

4. Trường hợp tổ chức cung cấp dịch vụ nhận lệnh của nhà đầu tư nước ngoài không cư trú tại Việt Nam thông qua hệ thống truyền lệnh trung gian do tổ chức nước ngoài cung cấp phải bảo đảm các yêu cầu sau:

a) Kết nối được thực hiện qua kênh truyền riêng, sử dụng giao thức theo chuẩn FIX hoặc tương đương, có cơ chế kiểm soát truy cập, bảo đảm an toàn bảo mật;

b) Có quy trình tiếp nhận, kiểm tra và xử lý lệnh;

c) Tổ chức cung cấp dịch vụ chịu trách nhiệm trước pháp luật về việc tiếp nhận, kiểm soát và xử lý lệnh giao dịch thông qua hệ thống truyền lệnh trung gian do tổ chức nước ngoài cung cấp.

Mục 2

TRIỂN KHAI GIAO DIỆN LẬP TRÌNH ỨNG DỤNG

Điều 14. Nguyên tắc triển khai API

1. Khi triển khai các dịch vụ API, tổ chức cung cấp dịch vụ phải tuân thủ quy định của pháp luật về chứng khoán, pháp luật về an ninh mạng. Trường hợp phát hiện dịch vụ API có nguy cơ gây rủi ro cho thị trường, tổ chức cung cấp dịch vụ phải dừng việc triển khai dịch vụ.

2. Tuân thủ các quy định của pháp luật về giữ bí mật, cung cấp thông tin khách hàng và bảo vệ dữ liệu cá nhân. Việc xử lý dữ liệu cá nhân của khách hàng chỉ phục vụ cho chính khách hàng đó, trừ trường hợp pháp luật có quy định khác.

3. Dữ liệu trong quá trình xử lý phải được quản lý, lưu trữ, khai thác, sử dụng đúng mục đích tại hợp đồng giữa các bên và phù hợp với quy định của pháp luật.

4. Dữ liệu trong quá trình xử lý phải bảo đảm tính cập nhật và chính xác. Trường hợp có sai lệch phải thực hiện đính chính, hiệu chỉnh kịp thời theo thỏa thuận giữa các bên.

5. Tổ chức cung cấp dịch vụ và bên thứ ba phải có hợp đồng về việc triển khai API. Hợp đồng phải có các nội dung sau:

a) Cam kết bảo đảm an toàn, bảo mật thông tin khi kết nối, xử lý dữ liệu; có biện pháp bảo vệ dữ liệu khách hàng;

b) Cam kết sử dụng dữ liệu được cung cấp đúng phạm vi, mục đích theo thỏa thuận giữa các bên, theo quy định của pháp luật và chịu trách nhiệm khi đề xảy ra rò rỉ, sai lệch hoặc sử dụng sai mục đích;

c) Thông tin về dịch vụ cung cấp cho khách hàng được triển khai qua API; yêu cầu bên thứ ba thông báo cho khách hàng các điều khoản, điều kiện sử dụng dịch vụ và hướng dẫn khách hàng cách thức sử dụng dịch vụ;

d) Thông tin về phí dịch vụ cung cấp cho khách hàng được triển khai qua API (nếu có);

đ) Điều khoản về hệ thống thông tin của bên thứ ba trước khi kết nối, xử lý dữ liệu qua API phải được đánh giá, xác định cấp độ theo quy định của pháp luật về bảo vệ an ninh mạng đối với hệ thống thông tin;

e) Quyền truy cập dữ liệu của các bên khi triển khai API;

g) Bên thứ ba phải thông báo cho tổ chức cung cấp dịch vụ khi phát hiện nhân sự vi phạm quy định về an ninh mạng khi triển khai API;

h) Trách nhiệm bồi thường của mỗi bên khi xảy ra rủi ro và trách nhiệm cung cấp thông tin, dữ liệu liên quan đến hoạt động triển khai API khi có yêu cầu của cơ quan có thẩm quyền;

i) Điều khoản chấm dứt hợp đồng.

6. Tổ chức cung cấp dịch vụ và bên thứ ba phải có hồ sơ kỹ thuật và hồ sơ phối hợp triển khai API, được lập và lưu giữ tại hai bên. Hồ sơ bao gồm các tài liệu có chứa nội dung sau:

a) Mô hình triển khai tại từng bên (sơ đồ luồng dữ liệu, phân vùng bảo mật, các điểm kết nối API);

b) Thông số kỹ thuật chi tiết (giao thức, điểm cuối, phiên bản, luồng dữ liệu, phương thức xác thực);

c) Cơ chế xác thực và phân quyền người dùng;

d) Cơ chế quản lý, kiểm soát và giới hạn tần suất truy cập;

đ) Hồ sơ, tài liệu triển khai các biện pháp bảo vệ an ninh mạng đối với hệ thống thông tin.

e) Các tài liệu khác có liên quan đến phối hợp triển khai API (nếu có).

Điều 15. Trách nhiệm của tổ chức cung cấp dịch vụ khi triển khai các dịch vụ API

1. Hoàn thiện cơ sở hạ tầng hệ thống thông tin phục vụ triển khai API để sẵn sàng kết nối, xử lý dữ liệu.

2. Xây dựng và ban hành các tài liệu hướng dẫn kết nối, xử lý dữ liệu.

3. Bảo đảm chất lượng dữ liệu trong quá trình triển khai API. Thông báo kịp thời cho bên thứ ba khi có sai lệch dữ liệu và phối hợp với bên thứ ba đính chính, hiệu chỉnh kịp thời.

4. Bảo đảm an ninh mạng cho hệ thống thông tin triển khai API, đáp ứng tối thiểu cấp độ bằng cấp độ của hệ thống giao dịch trực tuyến theo quy định của pháp luật về bảo vệ an ninh mạng đối với hệ thống thông tin.

5. Cung cấp công cụ hoặc chức năng cho phép khách hàng thực hiện các hoạt động sau:

a) Tra cứu các dữ liệu mà khách hàng đồng ý cho tổ chức cung cấp dịch vụ hoặc bên thứ ba xử lý;

b) Rút lại sự đồng ý của khách hàng theo quy định của pháp luật.

6. Thiết lập thời hạn được thực hiện truy vấn thông tin của khách hàng sau khi được khách hàng đồng ý không quá 180 ngày kể từ thời điểm hệ thống ghi nhận sự đồng ý của khách hàng, trừ trường hợp có thỏa thuận khác với khách hàng.

7. Kiểm soát truy cập API:

a) Tích hợp cơ chế quản lý, kiểm soát, giới hạn tần suất truy cập API (rate limit) nhằm giới hạn số lượng yêu cầu mà bên thứ ba có thể gửi trong một khoảng thời gian nhất định. Việc giới hạn tần suất truy cập thực hiện theo điểm b khoản này hoặc theo yêu cầu cụ thể của cơ quan có thẩm quyền;

b) Ban hành và công khai quy định về giới hạn tần suất truy cập API, trong đó phân mức giới hạn tần suất rõ ràng theo từng nhóm bên thứ ba. Việc phân mức này phải dựa trên những tiêu chí về lượng truy cập API thực tế và mức độ tuân thủ giới hạn của bên thứ ba;

c) Trong trường hợp bên thứ ba vượt quá giới hạn cho phép, tổ chức cung cấp dịch vụ tạm ngừng cung cấp dịch vụ qua API đối với bên thứ ba cho đến khi có biện pháp khắc phục;

d) Tích hợp cơ chế quản lý, kiểm soát, giới hạn số lượng địa chỉ IP truy cập API, thời gian truy cập API.

8. Triển khai hệ thống thử nghiệm API và công khai thông tin về hệ thống thử nghiệm API trên trang thông tin điện tử chính thức.

9. Chịu trách nhiệm lựa chọn, thẩm định, giám sát và quản lý bên thứ ba.

10. Tạm ngừng hoặc chấm dứt kết nối với bên thứ ba trong trường hợp phát hiện vi phạm quy định của pháp luật, vi phạm thỏa thuận hoặc có nguy cơ gây mất an toàn hệ thống.

11. Thực hiện cập nhật hoặc thu hồi quyền truy cập dữ liệu của bên thứ ba khi có thay đổi theo hợp đồng.

12. Giám sát hoạt động truy cập:

a) Có giải pháp giám sát để phát hiện và ngăn chặn các hành vi truy cập bất thường hoặc trái phép từ bên thứ ba;

b) Ghi nhật ký toàn bộ việc sử dụng API từ bên thứ ba để phục vụ kiểm tra khi cần thiết.

13. Cung cấp thông tin cho khách hàng về dịch vụ API triển khai và những rủi ro có thể gặp khi sử dụng.

14. Phối hợp với bên thứ ba theo hợp đồng và với cơ quan có thẩm quyền để giải quyết các tranh chấp, vướng mắc trong quá trình triển khai API.

15. Chịu trách nhiệm trước pháp luật về việc quản lý kết nối, cung cấp dịch vụ qua API đối với bên thứ ba.

Mục 3

HẠ TẦNG KỸ THUẬT, AN NINH BẢO MẬT THÔNG TIN VÀ LƯU TRỮ DỮ LIỆU CỦA HỆ THỐNG GIAO DỊCH TRỰC TUYẾN

Điều 16. Yêu cầu chung đối với công ty chứng khoán

1. Tuân thủ quy định về bảo vệ an ninh mạng đối với hệ thống thông tin theo quy định của pháp luật.

2. Trực tiếp quản lý, vận hành hệ thống.

3. Trang bị các thiết bị hạ tầng kỹ thuật công nghệ thông tin có bản quyền, nguồn gốc, xuất xứ rõ ràng. Có kế hoạch nâng cấp, thay thế các thiết bị sắp hết vòng đời sản phẩm và không được nhà xuất tiếp tục hỗ trợ, bảo đảm các trang thiết bị hạ tầng có khả năng cài đặt phiên bản phần mềm mới.

4. Kiểm tra, đánh giá an ninh mạng hệ thống giao dịch trực tuyến trước khi đưa vào khai thác, vận hành và định kỳ hàng năm. Việc kiểm tra, đánh giá được thực hiện bởi đơn vị có thẩm quyền kiểm tra, đánh giá an ninh mạng.

5. Sử dụng chứng thư số hợp lệ để xác thực trang thông tin điện tử, hệ thống thư điện tử.

6. Bố trí khu vực đặt hệ thống giao dịch trực tuyến phải bảo đảm các điều kiện về an ninh, môi trường và an toàn hệ thống như sau: là khu vực riêng biệt với các hệ thống khác. Có các hệ thống: hệ thống khóa từ hoặc thiết bị tương đương kiểm soát vào ra; hệ thống ghi hình; hệ thống báo cháy và chữa cháy chuyên dụng; hệ thống điều hoà không khí, theo dõi kiểm soát nhiệt độ và độ ẩm; hệ thống lưu điện và máy phát điện dự phòng chuyên dụng; hệ thống chống sét lan truyền.

7. Trường hợp thuê chỗ đặt hệ thống giao dịch trực tuyến tại các trung tâm dữ liệu (Data Center), các trung tâm dữ liệu này phải bảo đảm tuân thủ theo quy định của pháp luật Việt Nam về hoạt động của Data Center. Hệ thống giao dịch trực tuyến đặt tại Data Center phải có các giải pháp bảo đảm tránh truy cập và khai thác dữ liệu bất hợp pháp.

8. Ban hành quy trình, quy định về quản lý, vận hành hệ thống, nêu rõ trách nhiệm của đối tượng tham gia quy trình, bao gồm: Quy trình vận hành theo dõi quản trị hàng ngày; quy trình về xử lý sự cố; quy trình sao lưu dự phòng và khôi phục hệ thống, dữ liệu; quy trình kiểm soát rủi ro về hệ thống giao dịch, về cung cấp dịch vụ trực tuyến cho khách hàng; quy định về bảo vệ dữ liệu cá nhân và các quy trình, quy định khác phù hợp với quy định của pháp luật về giao dịch điện tử, pháp luật về an ninh mạng và quy định tại Thông tư này.

9. Xây dựng phương án đối phó, ứng cứu sự cố khẩn cấp về an ninh mạng cho hệ thống giao dịch trực tuyến.

10. Tách biệt môi trường vận hành hệ thống phần mềm giao dịch trực tuyến với các môi trường kiểm thử, phát triển phần mềm.

11. Sử dụng các máy chủ trung gian hoặc các hệ thống quản trị tập trung an toàn, có kiểm soát để thực hiện kết nối quản trị, giám sát và vận hành hệ thống; không sử dụng trực tiếp máy tính của nhân sự để quản trị, giám sát và vận hành.

12. Bố trí đội ngũ nhân viên có bằng cấp, chứng chỉ công nghệ thông tin về quản trị phần mềm, quản trị hệ thống và an ninh thông tin hoặc tương đương để quản lý và giám sát các hoạt động của hệ thống giao dịch trực tuyến bảo đảm liên tục và thông suốt.

13. Định kỳ hàng năm, tổ chức đào tạo, phổ biến, tuyên truyền nâng cao nhận thức và diễn tập về an ninh mạng cho cán bộ, nhân viên.

14. Có phương án dự phòng cho hệ thống giao dịch trực tuyến và cung cấp phương thức giao dịch thay thế trong trường hợp hệ thống giao dịch trực tuyến gặp sự cố.

Điều 17. Yêu cầu đối với hệ thống máy chủ của công ty chứng khoán

1. Có máy chủ dự phòng bảo đảm tính sẵn sàng cao.
2. Tách biệt về lô-gíc hoặc vật lý với các máy chủ hoạt động nghiệp vụ khác.
3. Có kiểm tra, tăng cường mức độ an toàn, bảo mật cho hệ điều hành, cập nhật các bản vá lỗi thường xuyên.
4. Có danh mục các phần mềm được phép cài đặt trên máy chủ. Định kỳ 06 tháng một lần thực hiện cập nhật, kiểm tra, bảo đảm tuân thủ danh mục này.

Điều 18. Yêu cầu đối với hệ thống phần mềm ứng dụng và cơ sở dữ liệu của công ty chứng khoán

1. Thực hiện quản lý các phiên bản phần mềm ứng dụng trực tuyến.
2. Các tính năng bắt buộc của phần mềm ứng dụng trực tuyến bao gồm:
 - a) Toàn bộ dữ liệu khi truyền trên môi trường mạng hoặc dữ liệu trao đổi giữa phần mềm ứng dụng trực tuyến với các trang thiết bị liên quan được áp dụng cơ chế mã hóa điểm đầu đến điểm cuối;
 - b) Có biện pháp bảo đảm tính toàn vẹn của dữ liệu giao dịch trong quá trình thực hiện giao dịch, lưu trữ dữ liệu;
 - c) Kiểm soát phiên đăng nhập: Hệ thống có cơ chế tự động ngắt phiên đăng nhập khi người sử dụng không thao tác trong một khoảng thời gian do công ty chứng khoán quy định hoặc áp dụng các biện pháp bảo vệ khác;
 - d) Có chức năng chống đăng nhập tự động;
 - đ) Có cơ chế giám sát, phát hiện và tự động ngăn chặn các hành vi truy cập, khai thác cơ sở dữ liệu trái phép hoặc vượt quyền; triển khai giải pháp phòng ngừa rò rỉ dữ liệu (Data Loss Prevention - DLP).
3. Phần mềm ứng dụng trực tuyến phải có chức năng lưu trữ các thông tin sau:
 - a) Thông tin định danh thiết bị di động hoặc thông tin định danh thiết bị máy tính: Thông tin định danh thiết bị di động là số IMEI hoặc Serial, hoặc WLAN MAC, hoặc Android ID hoặc thông tin định danh thiết bị di động khác. Thông tin định danh máy tính là địa chỉ MAC hoặc kết hợp các thông tin liên quan đến máy tính để định danh máy tính;

b) Nhật ký (log) giao dịch chứng khoán và giao dịch rút, chuyển tiền ra khỏi tài khoản giao dịch chứng khoán.

4. Nhật ký giao dịch chứng khoán gồm các thông tin sau: tên khách hàng, loại hình khách hàng, số tài khoản, thời gian nhận lệnh (ngày, giờ phút), mã chứng khoán, phương thức giao dịch, loại lệnh, số lượng và giá giao dịch, hình thức xác thực giao dịch, thời gian xác thực giao dịch, thông tin định danh thiết bị, địa chỉ IP mạng.

5. Nhật ký giao dịch rút, chuyển tiền ra khỏi tài khoản giao dịch chứng khoán gồm các thông tin sau: tên khách hàng, số tài khoản, số tiền, tài khoản ngân hàng nhận tiền, thời gian giao dịch, hình thức xác thực giao dịch, thông tin định danh thiết bị, địa chỉ IP mạng.

6. Phần mềm ứng dụng Mobile App tuân thủ quy định tại các khoản 1, 2, 3 Điều này và các yêu cầu sau:

a) Đăng ký và quản lý tại kho ứng dụng chính thức của hãng cung cấp hệ điều hành cho thiết bị di động;

b) Cài đặt trên thiết bị sử dụng số điện thoại di động đã được khách hàng đăng ký với công ty chứng khoán;

c) Có giải pháp nhằm phòng, chống, phát hiện các hành vi can thiệp trái phép vào ứng dụng giao dịch trực tuyến đã cài đặt trên thiết bị di động của khách hàng;

d) Không cho phép chức năng ghi nhớ mã khóa bí mật hoặc mã PIN truy cập;

đ) Khi khách hàng đăng nhập lần đầu hoặc đăng nhập trên thiết bị khác với thiết bị đã đăng nhập lần gần nhất phải thực hiện xác thực theo một trong các hình thức quy định tại Điều 7 Thông tư này.

7. Yêu cầu về cơ sở dữ liệu

a) Hệ quản trị cơ sở dữ liệu phải có bản quyền, có cơ chế bảo vệ và phân quyền truy cập đối với các tài nguyên cơ sở dữ liệu, phải được kiểm tra, nâng cao mức độ an toàn, bảo mật và cập nhật các bản vá lỗi thường xuyên;

b) Có biện pháp giám sát, ghi nhật ký truy cập cơ sở dữ liệu và các thao tác khi truy cập cơ sở dữ liệu.

Điều 19. Yêu cầu đối với hệ thống mạng, đường truyền, thiết bị của công ty chứng khoán

1. Trang bị tường lửa quản lý truy cập giữa các phân vùng. Thông tin khách hàng (thông tin nhận biết khách hàng, thông tin giao dịch của khách hàng)

không được lưu trữ tại phân vùng kết nối internet và phân vùng trung gian giữa mạng nội bộ và mạng internet (phân vùng DMZ).

2. Thiết lập chính sách hạn chế tối đa các dịch vụ mạng, cổng kết nối không sử dụng hoặc không cần thiết vào hệ thống giao dịch trực tuyến.

3. Kết nối từ bên ngoài mạng nội bộ vào hệ thống giao dịch trực tuyến để quản trị chỉ được thực hiện trong trường hợp không thể kết nối từ mạng nội bộ và phải tuân thủ các quy định sau:

a) Được cấp có thẩm quyền phê duyệt sau khi xem xét mục đích, cách thức kết nối;

b) Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn như sử dụng mạng riêng ảo hoặc phương án tương đương;

c) Thiết bị kết nối được cài đặt các phần mềm bảo đảm an toàn, bảo mật;

d) Áp dụng tối thiểu hai hình thức xác thực quy định Điều 7 Thông tư này khi đăng nhập hệ thống;

đ) Sử dụng giao thức truyền thông được mã hóa an toàn.

4. Trường hợp cung cấp phương thức đặt lệnh qua điện thoại, công ty chứng khoán phải trang bị hệ thống tổng đài hoặc thiết bị có chức năng ghi âm, quản lý, tra cứu cuộc gọi. Mọi cuộc gọi đặt lệnh của khách hàng phải được ghi âm, lưu trữ đầy đủ và phải bảo đảm an ninh mạng và bảo mật dữ liệu.

5. Đường truyền kết nối mạng cung cấp dịch vụ phải có dự phòng, bảo đảm tính sẵn sàng cao và khả năng cung cấp dịch vụ liên tục.

Điều 20. Yêu cầu về sao lưu, lưu trữ dữ liệu đối với công ty chứng khoán

1. Định kỳ thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống; bản dự phòng hệ điều hành máy chủ, hệ quản trị cơ sở dữ liệu; dữ liệu, thông tin liên quan đến giao dịch của khách hàng.

2. Có hệ thống hoặc phương tiện lưu trữ độc lập để sao lưu dự phòng. Dữ liệu sao lưu dự phòng phải được kiểm tra, bảo đảm khả năng khôi phục định kỳ sáu (06) tháng một lần và phải có biên bản xác nhận việc kiểm tra khôi phục dữ liệu. Biên bản xác nhận phải được lưu trữ tối thiểu ba (03) năm để phục vụ cho việc kiểm tra, đánh giá nội bộ hoặc kiểm toán (nếu có).

3. Các chứng từ điện tử, dữ liệu điện tử về giao dịch của khách hàng, thông tin của khách hàng phải được lưu trữ theo quy định của pháp luật.

4. Lưu trữ, bảo quản đầy đủ, chi tiết các thông tin sinh trắc học của khách hàng; kết quả đối chiếu thông tin sinh trắc học theo quy định tại khoản 6 Điều 9 Thông tư này.

5. Dữ liệu, cấu hình của hệ thống giao dịch trực tuyến, các thiết bị an toàn bảo mật phải được lưu trữ tối thiểu ba (03) bản, trong đó có hai (02) bản được lưu trên hai (02) thiết bị khác nhau, có một (01) bản được lưu độc lập đối với hệ thống giao dịch trực tuyến. Dữ liệu của hệ thống giao dịch trực tuyến phải được mã hóa trên thiết bị lưu trữ.

6. Thực hiện sao lưu hàng ngày đối với dữ liệu giao dịch, dữ liệu khách hàng; định kỳ sao lưu 01 tháng/01 lần đối với dữ liệu, cấu hình hệ thống giao dịch trực tuyến, cấu hình các thiết bị an toàn bảo mật.

7. Việc lưu trữ dữ liệu phải bảo đảm tính an toàn, bảo mật, đầy đủ và toàn vẹn của dữ liệu phục vụ cho công tác kiểm tra, đối chiếu, xác thực khách hàng trong quá trình sử dụng dịch vụ và cung cấp thông tin khi có yêu cầu của cơ quan có thẩm quyền.

Điều 21. Yêu cầu về hạ tầng kỹ thuật, an ninh bảo mật thông tin và lưu trữ dữ liệu của hệ thống giao dịch trực tuyến đối với công ty quản lý quỹ, đại lý phân phối chứng chỉ quỹ và các tổ chức có liên quan

1. Công ty quản lý quỹ, đại lý phân phối chứng chỉ quỹ cung cấp dịch vụ giao dịch trực tuyến phải xây dựng hệ thống bảo đảm tuân thủ quy định tại các khoản 1, 3, 5, 8, 9, 10, 11, 14 Điều 16; Điều 17; khoản 1, điểm a, b, c, d khoản 2, khoản 6, khoản 7 Điều 18; Điều 19 và Điều 20 Thông tư này.

2. Ngân hàng lưu ký, ngân hàng giám sát; đại lý ký danh; đại lý chuyển nhượng và các tổ chức có liên quan phải trang bị hạ tầng kỹ thuật phù hợp nếu cung cấp dịch vụ trực tuyến cho khách hàng, bảo đảm tuân thủ các quy định về an ninh mạng và lưu trữ dữ liệu, bảo mật dữ liệu khách hàng theo quy định tại Thông tư này.

Điều 22. Bảo mật dữ liệu khách hàng

Tổ chức cung cấp dịch vụ phải áp dụng các biện pháp bảo đảm an toàn, bảo mật dữ liệu khách hàng, tối thiểu bao gồm:

1. Dữ liệu khách hàng phải được bảo đảm an toàn, bảo mật theo quy định của pháp luật.

2. Thông tin sử dụng để xác thực giao dịch của khách hàng bao gồm yếu tố bí mật, thông tin sinh trắc học khi lưu trữ phải áp dụng các biện pháp mã hóa hoặc che dấu để bảo đảm tính bí mật.

3. Thiết lập quyền truy cập đúng chức năng, nhiệm vụ cho nhân sự thực hiện nhiệm vụ truy cập dữ liệu khách hàng; có biện pháp giám sát mỗi lần truy cập.

4. Có biện pháp quản lý truy cập, tiếp cận các thiết bị, phương tiện lưu trữ dữ liệu của khách hàng để phòng chống nguy cơ lộ, lọt dữ liệu.

5. Thông báo cho khách hàng khi xảy ra sự cố làm lộ, lọt dữ liệu của khách hàng và báo cáo kịp thời về Ủy ban Chứng khoán Nhà nước.

Chương III

HOẠT ĐỘNG TRAO ĐỔI THÔNG TIN ĐIỆN TỬ VÀ CHẾ ĐỘ BẢO CÁO, CÔNG BỐ THÔNG TIN

Điều 23. Hoạt động trao đổi thông tin điện tử trên thị trường chứng khoán

1. Nội dung trao đổi thông tin điện tử trên thị trường chứng khoán bao gồm thông tin liên quan đến các hoạt động sau:

a) Chào bán chứng khoán ra công chúng, đăng ký chứng khoán, lưu ký chứng khoán, niêm yết, đăng ký giao dịch và giao dịch chứng khoán;

b) Hoạt động quản lý các tổ chức, cá nhân theo quy định tại khoản 2 Điều 2 Thông tư này;

c) Hoạt động công bố thông tin trên thị trường chứng khoán;

d) Hoạt động khác liên quan đến thị trường chứng khoán theo quy định của pháp luật chứng khoán.

2. Tổ chức cung cấp dịch vụ trao đổi thông tin điện tử có trách nhiệm:

a) Tạo lập trang thông tin điện tử đóng vai trò như một cổng vào cho dịch vụ trao đổi thông tin điện tử;

b) Bảo mật thông tin cho các đối tượng đăng ký sử dụng dịch vụ và bảo đảm an ninh mạng cho hệ thống trao đổi thông tin điện tử;

c) Ban hành quy chế hướng dẫn về dịch vụ trao đổi thông tin điện tử.

3. Đối tượng tham gia trao đổi thông tin điện tử đăng ký sử dụng dịch vụ và thực hiện theo quy chế hướng dẫn của tổ chức cung cấp dịch vụ trao đổi thông tin điện tử.

4. Việc sử dụng chứng thư số, chữ ký số trong hoạt động trao đổi thông tin điện tử được thực hiện theo quy định của pháp luật về giao dịch điện tử trong hoạt động tài chính.

Điều 24. Các hoạt động khác có liên quan đến giao dịch điện tử trên thị trường chứng khoán

Các hoạt động khác có liên quan đến giao dịch điện tử trên thị trường chứng khoán thực hiện theo quy định tại Thông tư này và quy định pháp luật về giao dịch điện tử trong hoạt động tài chính.

Điều 25. Chế độ báo cáo trong cung cấp dịch vụ trực tuyến

1. Công ty chứng khoán được chấp thuận cung cấp dịch vụ giao dịch chứng khoán trực tuyến phải gửi Ủy ban Chứng khoán Nhà nước các báo cáo sau:

a) Báo cáo năm về hoạt động cung cấp dịch vụ trực tuyến theo mẫu quy định tại Phụ lục II ban hành kèm theo Thông tư này kèm theo báo cáo về việc kiểm tra, đánh giá an ninh mạng định kỳ. Thời hạn nộp báo cáo chậm nhất là ngày 31 tháng 01 năm tiếp theo;

b) Báo cáo kèm theo các tài liệu liên quan khi có nâng cấp, thay đổi hệ thống giao dịch trực tuyến: Thay đổi core hệ thống, thay đổi người quản lý hệ thống, thay đổi địa điểm đặt hệ thống, thay đổi địa chỉ website hoặc tên phần mềm cung cấp dịch vụ giao dịch trực tuyến theo mẫu quy định tại Phụ lục VIII ban hành kèm theo Thông tư này. Báo cáo nộp trong thời hạn bảy (07) ngày làm việc sau khi công ty chứng khoán thực hiện thay đổi;

2. Tổ chức cung cấp dịch vụ triển khai các API phải báo cáo Ủy ban Chứng khoán Nhà nước theo mẫu quy định tại Phụ lục III ban hành kèm theo Thông tư này. Thời hạn nộp báo cáo tối thiểu bảy (07) ngày làm việc trước khi thực hiện.

3. Sở giao dịch chứng khoán Việt Nam gửi Ủy ban Chứng khoán Nhà nước báo cáo năm về việc quản lý, vận hành hệ thống giao dịch chứng khoán theo mẫu quy định tại Phụ lục IV ban hành kèm theo Thông tư này. Thời hạn nộp báo cáo chậm nhất là ngày 31 tháng 01 năm tiếp theo;

4. Tổng công ty lưu ký và bù trừ chứng khoán Việt Nam gửi Ủy ban Chứng khoán Nhà nước báo cáo năm liên quan đến quản lý, vận hành cổng giao tiếp trực tuyến, cổng giao tiếp điện tử với thành viên, hệ thống khác có liên quan theo mẫu quy định tại Phụ lục V ban hành kèm theo Thông tư này. Thời hạn nộp báo cáo chậm nhất là ngày 31 tháng 01 năm tiếp theo.

5. Trong thời hạn hai mươi bốn (24) giờ kể từ khi xảy ra các sự cố nghiêm trọng, tổ chức cung cấp dịch vụ phải gửi báo cáo theo mẫu quy định tại Phụ lục VI ban hành kèm theo Thông tư này.

6. Trong thời hạn hai mươi bốn (24) giờ kể từ khi xảy ra các sự cố nghiêm trọng, Sở giao dịch chứng khoán Việt Nam và công ty con, Tổng công ty lưu ký

và bù trừ chứng khoán Việt Nam và công ty con phải gửi báo cáo theo mẫu quy định tại Phụ lục VII ban hành kèm theo Thông tư này.

7. Trường hợp xảy ra sự cố nghiêm trọng về an ninh mạng vượt ngoài khả năng xử lý, tổ chức cung cấp dịch vụ, Sở giao dịch chứng khoán Việt Nam và công ty con, Tổng công ty lưu ký và bù trừ chứng khoán Việt Nam và công ty con phải kịp thời báo cáo cơ quan chuyên trách theo quy định của pháp luật về an ninh mạng.

8. Công ty quản lý quỹ, đại lý phân phối chứng chỉ quỹ phải báo cáo Ủy ban Chứng khoán Nhà nước tài liệu theo mẫu quy định tại Phụ lục I ban hành kèm theo Thông tư này trong thời hạn tối thiểu năm (05) ngày làm việc trước ngày triển khai hệ thống giao dịch trực tuyến cho khách hàng; thực hiện báo cáo năm về hoạt động cung cấp dịch vụ trực tuyến theo mẫu quy định tại Phụ lục II ban hành kèm theo Thông tư này, thời hạn nộp báo cáo chậm nhất là ngày 31 tháng 01 năm tiếp theo.

9. Báo cáo gửi bằng phương thức điện tử thực hiện theo hướng dẫn của Ủy ban Chứng khoán Nhà nước. Căn cứ yêu cầu quản lý và sự phát triển về dịch vụ trực tuyến của thị trường chứng khoán, Ủy ban Chứng khoán Nhà nước hướng dẫn báo cáo về nội dung khác tại mục 5 Phụ lục I, mục 11 Phụ lục II, mục 6 Phụ lục III, mục 8 Phụ lục IV, mục 3 Phụ lục V, mục 7 Phụ lục VI, mục 9 Phụ lục VII, mục 5 Phụ lục VIII Thông tư này.

Điều 26. Công bố thông tin trong cung cấp dịch vụ trực tuyến

1. Trang thông tin điện tử chính thức và phần mềm ứng dụng chứng khoán trực tuyến của tổ chức cung cấp dịch vụ phải công bố các quy định về dịch vụ trực tuyến, những rủi ro có thể xảy ra khi khách hàng thực hiện dịch vụ trực tuyến và trách nhiệm bồi thường của mỗi bên khi xảy ra rủi ro. Các rủi ro bao gồm:

a) Trong khi truyền tải qua mạng internet, lệnh giao dịch có thể bị treo, bị ngừng, bị trì hoãn hoặc có lỗi dữ liệu;

b) Việc nhận dạng các tổ chức hoặc khách hàng có thể không chính xác, lỗi về bảo mật có thể xảy ra;

c) Giá cả thị trường và các thông tin chứng khoán khác có thể có lỗi hoặc sai lệch;

d) Các rủi ro có thể xảy ra của các phương thức xác thực đặt lệnh cho khách hàng;

đ) Các rủi ro khác mà các cơ quan quản lý nhà nước có thẩm quyền, tổ chức cung cấp dịch vụ thấy cần thiết phải công bố.

2. Tổ chức cung cấp dịch vụ phải công khai danh mục các dịch vụ API đang triển khai (nếu có) để cung cấp dịch vụ trực tuyến trên trang thông tin điện tử của tổ chức, bao gồm các nội dung sau:

- a) Tên dịch vụ và mô tả chức năng;
- b) Phạm vi dữ liệu được truy cập;
- c) Thông tin về hình thức xác thực và bảo mật;
- d) Danh sách các bên thứ ba được phép truy cập hợp pháp (nếu có).
- đ) Các nội dung khác có liên quan đến dịch vụ API đang triển khai (nếu có).

3. Sở giao dịch chứng khoán Việt Nam và công ty con công bố trên trang thông tin điện tử của Sở giao dịch chứng khoán Việt Nam và công ty con quy định pháp luật liên quan đến giao dịch điện tử trên thị trường chứng khoán và các văn bản quy định về hoạt động giao dịch điện tử do Sở giao dịch chứng khoán Việt Nam và công ty con ban hành.

4. Tổng công ty lưu ký và bù trừ chứng khoán Việt Nam và công ty con công bố trên trang thông tin điện tử của Tổng công ty lưu ký và bù trừ chứng khoán Việt Nam và công ty con danh sách các sản phẩm, dịch vụ được phép cung cấp; quy định pháp luật liên quan đến giao dịch điện tử trên thị trường chứng khoán và các văn bản quy định về hoạt động giao dịch điện tử do Tổng công ty lưu ký và bù trừ chứng khoán Việt Nam và công ty con ban hành.

5. Ủy ban Chứng khoán Nhà nước đăng tải trên cổng thông tin điện tử Ủy ban Chứng khoán Nhà nước danh sách công ty chứng khoán được phép cung cấp dịch vụ giao dịch chứng khoán trực tuyến.

Chương IV

TRÁCH NHIỆM CỦA CÁC CƠ QUAN, TỔ CHỨC, CÁ NHÂN THAM GIA HOẠT ĐỘNG GIAO DỊCH ĐIỆN TỬ TRÊN THỊ TRƯỜNG CHỨNG KHOÁN

Điều 27. Trách nhiệm của các tổ chức, cá nhân tham gia hoạt động giao dịch điện tử trên thị trường chứng khoán

- 1. Tuân thủ quy định trong hoạt động giao dịch chứng khoán và thị trường chứng khoán.
- 2. Tuân thủ quy định của pháp luật về giao dịch điện tử, an ninh mạng, bảo vệ dữ liệu cá nhân và quy định khác của pháp luật có liên quan.

3. Thực hiện lưu giữ đầy đủ hồ sơ, tài liệu chứng từ liên quan đến hoạt động giao dịch trực tuyến của đơn vị. Thực hiện lưu giữ thông tin đã báo cáo theo quy định của pháp luật.

4. Công ty chứng khoán không được cung cấp dịch vụ giao dịch chứng khoán trực tuyến khi chưa được Ủy ban Chứng khoán Nhà nước chấp thuận hoặc khi quyết định chấp thuận bị thu hồi.

5. Thực hiện báo cáo đúng thời hạn, báo cáo đầy đủ nội dung theo quy định của pháp luật hoặc theo yêu cầu của Ủy ban Chứng khoán Nhà nước.

Điều 28. Trách nhiệm kiểm tra, giám sát hoạt động giao dịch điện tử trên thị trường chứng khoán

1. Ủy ban Chứng khoán Nhà nước có trách nhiệm giám sát, kiểm tra định kỳ hoặc bất thường đối với Sở giao dịch chứng khoán Việt Nam và công ty con, Tổng công ty lưu ký và bù trừ chứng khoán Việt Nam và công ty con, các tổ chức cung cấp dịch vụ và các tổ chức, cá nhân khác về thực hiện giao dịch điện tử trên thị trường chứng khoán theo quy định hoặc khi xảy ra sự cố ảnh hưởng đến quyền lợi của khách hàng và sự an toàn của thị trường chứng khoán.

2. Sở giao dịch chứng khoán Việt Nam và công ty con, Tổng công ty lưu ký và bù trừ chứng khoán Việt Nam và công ty con có trách nhiệm phối hợp giám sát hoạt động giao dịch chứng khoán trực tuyến của tổ chức cung cấp dịch vụ và các tổ chức, cá nhân có liên quan theo yêu cầu của Ủy ban Chứng khoán Nhà nước.

3. Tổ chức cung cấp dịch vụ khi triển khai API có trách nhiệm giám sát bên thứ ba theo quy định tại khoản 9 Điều 15 Thông tư này.

4. Tổ chức, cá nhân tham gia giao dịch điện tử trên thị trường chứng khoán có trách nhiệm cung cấp đầy đủ, kịp thời thông tin, dữ liệu và các tài liệu liên quan đến hoạt động giao dịch điện tử khi có yêu cầu của cơ quan có thẩm quyền.

Điều 29. Trách nhiệm xây dựng quy trình, quy chế về giao dịch điện tử trên thị trường chứng khoán

1. Sở giao dịch chứng khoán Việt Nam ban hành các quy chế nghiệp vụ quy định:

a) Kết nối hệ thống từ thành viên đến hệ thống giao dịch chứng khoán của Sở giao dịch chứng khoán Việt Nam phù hợp với Luật chứng khoán, Luật Giao dịch điện tử, Luật An ninh mạng, các văn bản hướng dẫn thi hành và quy định tại Thông tư này.

b) Biện pháp giới hạn giao dịch tối đa tại một thời điểm (nếu cần thiết) áp dụng cho các thành viên để phù hợp với hệ thống giao dịch chứng khoán của Sở giao dịch chứng khoán Việt Nam và công ty con.

2. Tổng công ty lưu ký và bù trừ chứng khoán Việt Nam ban hành quy chế nghiệp vụ về kết nối hệ thống từ thành viên đến các cổng giao tiếp trực tuyến, cổng giao tiếp điện tử phù hợp với Luật chứng khoán, Luật Giao dịch điện tử, Luật An ninh mạng, các văn bản hướng dẫn thi hành và quy định tại Thông tư này.

3. Tổ chức cung cấp dịch vụ ban hành quy trình, quy chế về giao dịch điện tử theo quy định tại khoản 5 Điều 5, khoản 8 Điều 16 Thông tư này.

Chương V

ĐIỀU KHOẢN THI HÀNH

Điều 30. Hiệu lực thi hành

Thông tư này có hiệu lực thi hành kể từ ngày tháng năm 2026 và thay thế 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 của Bộ trưởng Bộ Tài chính 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.

Điều 31. Điều khoản chuyển tiếp

1. Các tổ chức cung cấp dịch vụ đã kết nối, xử lý dữ liệu với bên thứ ba qua API có trách nhiệm lập danh mục các API đang triển khai và thông tin chi tiết bảo đảm tuân thủ các quy định của Thông tư này gửi Ủy ban Chứng khoán Nhà nước trong thời hạn 03 tháng kể từ ngày Thông tư này có hiệu lực thi hành.

2. Tổ chức cung cấp dịch vụ có trách nhiệm rà soát, lập kế hoạch, hoàn thiện hệ thống, dữ liệu của khách hàng bảo đảm tuân thủ quy định tại Thông tư này trong thời hạn 01 năm kể từ ngày Thông tư này có hiệu lực thi hành.

Điều 32. Tổ chức thực hiện

1. Ủy ban Chứng khoán Nhà nước, Sở giao dịch chứng khoán Việt Nam và công ty con, Tổng công ty lưu ký và bù trừ chứng khoán Việt Nam và công ty con và các tổ chức, cá nhân tham gia giao dịch điện tử trên thị trường chứng khoán chịu trách nhiệm thi hành Thông tư này.

2. Trường hợp các văn bản dẫn chiếu tại Thông tư này được sửa đổi, bổ sung hoặc thay thế thì thực hiện theo các văn bản sửa đổi, bổ sung hoặc thay thế.

3. Trong quá trình thực hiện, nếu có vướng mắc đề nghị các tổ chức, cá nhân có liên quan phản ánh về Bộ Tài chính để nghiên cứu, hướng dẫn, giải quyết.

Nơi nhận:

- Ban Bí thư Trung ương Đảng;
- Văn phòng Trung ương và các Ban của Đảng;
- Văn phòng Tổng Bí thư;
- Văn phòng Chính phủ;
- Văn phòng Quốc hội;
- Văn phòng Chủ tịch nước;
- Thủ tướng, các Phó thủ tướng Chính phủ;
- Ủy ban Trung ương Mặt trận Tổ quốc Việt Nam;
- Hội đồng dân tộc và các Ủy ban của Quốc hội;
- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- HĐND, UBND các tỉnh, thành phố trực thuộc TW;
- Viện Kiểm sát nhân dân tối cao;
- Tòa án nhân dân tối cao;
- Kiểm toán Nhà nước;
- Cơ quan Trung ương của các đoàn thể;
- Cục kiểm tra văn bản và Quản lý xử lý vi phạm hành chính (Bộ Tư pháp);
- Liên đoàn thương mại và công nghiệp Việt Nam;
- Bộ trưởng Bộ Tài chính (để báo cáo);
- Các đơn vị thuộc Bộ Tài chính;
- Công báo;
- Cơ sở dữ liệu quốc gia về pháp luật;
- Cổng thông tin điện tử Chính phủ;
- Cổng thông tin điện tử Bộ Tài chính;
- Cổng thông tin điện tử Ủy ban Chứng khoán Nhà nước;
- Các Sở GD&ĐT, TCTLKB&ĐT;
- Lưu: VT, UBCK (150b).

**KT. BỘ TRƯỞNG
THỨ TRƯỞNG**

Nguyễn Đức Chi

Phụ lục I

BÁO CÁO THIẾT KẾ HỆ THỐNG GIAO DỊCH TRỰC TUYẾN

(Ban hành kèm theo Thông tư số /2026/TT-BTC ngày tháng năm 2026 của Bộ trưởng Bộ Tài chính quy định giao dịch điện tử trên thị trường chứng khoán)

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

... , ngày... tháng... năm ...

BÁO CÁO THIẾT KẾ HỆ THỐNG GIAO DỊCH TRỰC TUYẾN

Kính gửi: Ủy ban Chứng khoán Nhà nước

I. Thông tin báo cáo

Tên tổ chức cung cấp dịch vụ:.....

Ngày lập báo cáo:.....

Người lập báo cáo:.....

Email liên hệ:.....

Điện thoại di động:.....

II. Hệ thống giao dịch trực tuyến

1. Tổng quan về hệ thống giao dịch trực tuyến (GDTT)

1.1. Phương thức giao dịch cung cấp

Web Trading ☐

Mobile App Trading ☐

Điện thoại (Call Center) ☐

API Trading ☐

Khác ☐

Mô tả về phương thức giao dịch cung cấp nếu chọn “Khác”:.....

1.2. Quy trình giao dịch

Các quy trình GDTT đã ban hành:

STT	Tên quy trình	Ngày ban hành
1		

STT	Tên quy trình	Ngày ban hành
2		
...		

Đính kèm các quy trình đã ban hành.

1.3. Địa điểm đặt hệ thống GDTT

2. Giải pháp xây dựng hạ tầng kỹ thuật hệ thống GDTT

2.1. Giải pháp xây dựng hệ thống

- Kiến trúc và mô hình hệ thống mạng GDTT:

Số phân vùng	
Có Data Center riêng	Có ☐ Không ☐
Thuê đặt Data center	Có ☐ Không ☐
Có DR Site	Có ☐ Không ☐
Mô hình DR	Active-Active ☐ Active-Passive ☐
Có phân vùng DMZ cho hệ thống giao dịch	Có ☐ Không ☐
Có phân vùng mạng riêng cho cơ sở dữ liệu	Có ☐ Không ☐
Có phân tách vùng mạng quản trị (Management Network)	Có ☐ Không ☐
Có hệ thống cân bằng tải (Load Balancer)	Có ☐ Không ☐

Đính kèm sơ đồ kiến trúc hệ thống kèm theo các thuyết minh chi tiết.

- Hệ thống máy chủ:

STT	Tên máy chủ	Số lượng	Mô tả chức năng	Nhà cung cấp
1				
2				
...				

- Đường truyền mạng:

STT	Tên đường truyền	Dung lượng	Mô tả chức năng	Nhà cung cấp
1				
2				
....				

- Thiết bị hệ thống mạng và hệ thống phụ trợ liên quan đến hệ thống GDCKTT:

STT	Tên thiết bị	Số lượng	Mô tả chức năng	Nhà cung cấp
1				
2				
...				

- Hệ thống tổng đài điện thoại (nếu công ty cung cấp phương thức đặt lệnh qua điện thoại):

Tên hệ thống tổng đài	
-----------------------	--

Số lượng tổng đài	
Nhà cung cấp	
Phần mềm giao dịch điện thoại	
Số kênh cuộc gọi đồng thời	
Có ghi âm cuộc gọi	Có ☐ Không ☐
Thời gian lưu file ghi âm	
Có sử dụng IVR (Interactive Voice Response - hệ thống trả lời thoại tự động)	Có ☐ Không ☐
Có xác thực khách hàng qua IVR	Có ☐ Không ☐

2.2. Giải pháp an ninh bảo mật của hệ thống

a) Bảo mật hạ tầng mạng:

Có tường lửa mạng (Firewall)	Có ☐ Không ☐
Số lượng Firewall	
Có hệ thống IDS/IPS	Có ☐ Không ☐
Có hệ thống chống tấn công DDoS	Có ☐ Không ☐
Có hệ thống WAF	Có ☐ Không ☐
SIEM	Có ☐ Không ☐
SOC	Có ☐ Không ☐
Khác	

Đính kèm mô tả cách thức tổ chức để bảo đảm an toàn bảo mật.

b) Bảo mật ứng dụng:

Sử dụng giao thức HTTPS/TLS	Có ☐ Không ☐
Phiên bản TLS sử dụng	TLS 1.2 ☐ TLS 1.3 ☐ Khác:
Có vô hiệu hóa TLS 1.0 và TLS 1.1	Có ☐ Không ☐
Có kiểm soát truy cập API	Có ☐ Không ☐
Có bảo vệ chống SQL Injection	Có ☐ Không ☐
Thuật toán mã hóa sử dụng (AES, RSA,...)	
Có xác thực chống giả mạo domain (phishing)	Có ☐ Không ☐

c) Chính sách bảo mật

Có ban hành chính sách an toàn thông tin	Có ☐ Không ☐
Có chính sách quản lý truy cập	Có ☐ Không ☐
Có thực hiện kiểm thử xâm nhập (Pentest) trước khi đưa vào vận hành	Có ☐ Không ☐
Đơn vị kiểm thử	Nội bộ ☐ Thuê ngoài ☐
Đơn vị thuê thực hiện kiểm thử	
Thời điểm kiểm thử gần nhất	

Có lưu log truy cập hệ thống	Có ☐ Không ☐
Thời gian lưu log (năm)	
Kiểm soát cổng kết nối ngoại vi	Có ☐ Không ☐

Đính kèm báo cáo Pentest, các chính sách bảo mật đã ban hành

d) Xác thực giao dịch

- Xác thực giao dịch chứng khoán:

Có xác thực sinh trắc học	Có ☐ Không ☐
Loại sinh trắc học sử dụng	Vân tay ☐ Khuôn mặt ☐ Giọng nói ☐ Khác:
Mục đích sử dụng	Đăng nhập tài khoản ☐ Xác thực lệnh ☐ Khác:
Nhà cung cấp giải pháp	
Có đối chiếu dữ liệu sinh trắc học với CSDLQG dân cư	Có ☐ Không ☐

Đính kèm Quy trình thu thập dữ liệu sinh trắc học

- Xác thực giao dịch tiền

Ngưỡng giao dịch	Phương thức xác thực
Dưới 10 triệu đồng	Sinh trắc học ☐ SMS OTP ☐ Voice OTP ☐ Email OTP ☐ ☐ Soft OTP ☐ Token OTP ☐ FIDO ☐ Chữ ký số ☐ Xác thực hai kênh ☐ Khác:...
Từ 10 triệu đồng trở lên	Sinh trắc học: Có ☐ Không ☐

đ) Chính sách truy cập từ xa

Cho phép truy cập từ xa	Có ☐ Không ☐
Phương thức truy cập	VPN ☐ SSH ☐ Khác:
Hình thức xác thực	Mật khẩu ☐ OTP ☐ Sinh trắc học ☐ Chứng thư số ☐ Khác:...
Xác thực đa yếu tố (MFA)	Có ☐ Không ☐
Giới hạn IP truy cập	Có ☐ Không ☐
Giám sát phiên truy cập (Log chi tiết thời gian, user, địa chỉ IP, hoạt động thực hiện,...)	Có ☐ Không ☐
Thời gian truy cập cho phép	
Tắt truy cập khi không dùng	Có ☐ Không ☐

3. Phần mềm giao dịch

a) Thông tin phần mềm

Website giao dịch	
Tên mobile app	
Đăng ký trên Android/iOS	Có ☐ Không ☐

Nhà cung cấp	
Công nghệ phát triển	(Java, .NET, Python, Node.js, PHP, Khác)
Hệ điều hành server	(Windows Server/Linux (Ubuntu/CentOS)/Unix/Khác)
CSDL sử dụng	(Oracle/SQL Server/PostgreSQL/MySQL/Khác)

b) Các chức năng chính của phần mềm:

(Mô tả các chức năng chính của phần mềm)

c) Lưu trữ thông tin định danh thiết bị:

Đối với website:

Đối với mobile app:

d) Nhật ký giao dịch:

- Lưu nhật ký giao dịch: Có ☐ Không ☐

Thông tin lưu trữ đối với giao dịch chứng khoán:

Thông tin lưu trữ đối với giao dịch tiền:

- Thời gian lưu trữ (năm):

e) Các giải pháp bảo mật của phần mềm:

(Mô tả các giải pháp bảo mật của phần mềm)

4. Hệ thống dự phòng

4.1. Dự phòng dữ liệu

Có triển khai dự phòng dữ liệu	Có ☐ Không ☐
Tần suất backup	Hàng ngày ☐ , hàng giờ ☐ , real-time ☐ khác ☐ (...)
Thời gian lưu trữ dữ liệu dự phòng	
Kiểm thử khôi phục dữ liệu	Có ☐ Không ☐
Thời gian khôi phục (RTO)	
Có lưu trữ dữ liệu theo quy tắc 3-2-1	Có ☐ Không ☐

Đính kèm mô tả chi tiết về giải pháp dự phòng dữ liệu

4.2. Giải pháp thiết kế dự phòng cho hệ thống GDCKTT

a) Dự phòng cho hệ thống máy chủ

Có triển khai dự phòng máy chủ	Có ☐ Không ☐
Mô hình dự phòng	Active-Active ☐ Active-Passive ☐
Số lượng máy chủ chính (Primary)	
Số lượng máy chủ dự phòng	
Có cơ chế failover tự động	Có ☐ Không ☐
Thời gian chuyển đổi (Failover time)	
Kiểm tra failover định kỳ	(Hàng tháng/Hàng quý/Hàng năm)
Có server dự phòng tại DR	Có ☐ Không ☐
Số lượng server tại DR	

Cơ chế đồng bộ dữ liệu với DR	
-------------------------------	--

b) Dự phòng hệ thống mạng, đường truyền, thiết bị

- Dự phòng hệ thống mạng

Có cơ chế failover tự động	Có ☐ Không ☐
Thời gian chuyển đổi	
Có load balancing mạng	Có ☐ Không ☐
Thiết bị/công nghệ load balancer	Hardware Load Balancer ☐
	Software Load Balancer ☐
	Cloud Load Balancer ☐
	Khác:
Có đường truyền DC – DR riêng	Có ☐ Không ☐
Số đường truyền DC – DR	
Bảng thông kết nối DC – DR	
Công nghệ kết nối	MPLS ☐
	Metro Ethernet ☐
	Dedicated Fiber ☐
	Khác ☐

- Dự phòng đường truyền:

Có đường truyền dự phòng	Có ☐ Không ☐
Đường truyền chính và dự phòng có sử dụng của hai nhà cung cấp khác nhau	Có ☐ Không ☐
Mô hình dự phòng đường truyền	Active–Active ☐ Active–Standby ☐

- Dự phòng thiết bị mạng

Dự phòng router	Có ☐ Không ☐
Dự phòng switch core	Có ☐ Không ☐
Dự phòng firewall	Có ☐ Không ☐
Mô hình dự phòng thiết bị	Active–Active ☐ Active–Passive ☐

c) Dự phòng hệ thống tổng đài điện thoại (nếu công ty cung cấp phương thức đặt lệnh qua điện thoại)

Có tổng đài dự phòng	Có ☐ Không ☐
Mô hình dự phòng	Active–Active ☐
	Active–Standby ☐
Số lượng SIP trunk / đường trung kế	
Có đường truyền thoại dự phòng	Có ☐ Không ☐
Có chuyển hướng cuộc gọi khi tổng đài lỗi	Có ☐ Không ☐
Phương án chuyển hướng	Sang tổng đài dự phòng ☐
	Sang hotline di động ☐

	Sang contact center cloud ☐
	Khác ☐

4.3. Hệ thống điện

Có UPS cho hệ thống GDCKTT	Có ☐ Không ☐
Số lượng UPS	
Công suất UPS	
Thời gian duy trì khi mất điện	
Có máy phát điện dự phòng	Có ☐ Không ☐
Số lượng máy phát điện	
Công suất máy phát	
Thời gian khởi động máy phát	
Thời gian duy trì hoạt động	
Thời gian chuyển đổi sang máy phát	
Kiểm tra máy phát điện định kỳ	(Hàng tháng/Hàng quý/Hàng năm)
Kiểm tra UPS định kỳ	(Hàng tháng/Hàng quý/Hàng năm)

4.4. Giải pháp kiểm soát an ninh phòng máy chủ

Có hệ thống kiểm soát ra vào	Có ☐ Không ☐
Phương thức xác thực	(Thẻ từ/vân tay/khuôn mặt/mã PIN)
Có nhật ký ra vào phòng máy	Có ☐ Không ☐
Thời gian lưu nhật ký	
Có phân quyền vào ra theo vai trò	Có ☐ Không ☐
Có khóa tủ rack	Có ☐ Không ☐
Có hệ thống cảnh báo xâm nhập	Có ☐ Không ☐
Cơ chế cảnh báo	Báo động ☐ SMS ☐ Email ☐ Hệ thống giám sát SOC/NOC ☐
Có camera giám sát phòng máy	Có ☐ Không ☐
Vị trí camera	Cửa ra vào ☐
	Bên trong phòng máy ☐
	Hành lang ☐
	Khu vực tủ rack ☐
Có ghi hình 24/7	Có ☐ Không ☐
Thời gian lưu trữ video	

4.4. Hệ thống phụ trợ

- Hệ thống chống sét:

Có hệ thống chống sét trực tiếp cho tòa nhà/phòng máy ☐ Có ☐ Không ☐

Có thiết bị chống sét lan truyền ☐ Có ☐ Không ☐

- Hệ thống làm mát

Có hệ thống điều hòa phòng máy chuyên dụng	Có ☐ Không ☐
Số lượng thiết bị làm mát	
Công suất mỗi thiết bị	
Mô hình dự phòng	
Có hệ thống giám sát nhiệt độ phòng máy	Có ☐ Không ☐
Có hệ thống giám sát độ ẩm	Có ☐ Không ☐
Có cảnh báo khi vượt ngưỡng	Có ☐ Không ☐
Hình thức cảnh báo	SMS
	Email
	Hệ thống giám sát NOC

- Hệ thống phòng cháy chữa cháy:

Có hệ thống phát hiện cháy tự động	Có ☐ Không ☐
Loại cảm biến	Cảm biến khói ☐
	Cảm biến nhiệt ☐
	Hệ thống phát hiện khói sớm (VESDA)
Có hệ thống chữa cháy tự động cho phòng máy chủ	Có ☐ Không ☐
Loại hệ thống chữa cháy	Khí FM200 ☐
	Khí Novec 1230 ☐
	Khí CO2 ☐
	Hệ thống khác ☐
Có hệ thống chữa cháy cầm tay	Có ☐ Không ☐
Kiểm tra hệ thống PCCC định kỳ	Có ☐ Không ☐
Tần suất kiểm tra	Hàng tháng ☐
	Hàng quý ☐
	Hàng năm ☐
Có hồ sơ kiểm định PCCC	Có ☐ Không ☐

4.5. Bảo trì định kỳ hệ thống

Có ban hành kế hoạch bảo trì hệ thống CNTT	Có ☐ Không ☐
Đơn vị thực hiện bảo trì	(Nội bộ / Nhà cung cấp / Kết hợp)
Có hợp đồng bảo trì với nhà cung cấp	Có ☐ Không ☐
Tần suất bảo trì định kỳ	Hàng tháng ☐
	Hàng quý ☐
	Hàng năm ☐
Kiểm tra tình trạng hoạt động thiết bị	Có ☐ Không ☐
Kiểm tra cảnh báo hệ thống	Có ☐ Không ☐

Vệ sinh thiết bị	Có ☐ Không ☐
Kiểm tra firmware/software	Có ☐ Không ☐
Cập nhật bản vá bảo mật	Có ☐ Không ☐
Kiểm tra khả năng dự phòng hệ thống	Có ☐ Không ☐

4.6. Nhân sự vận hành hệ thống

Có bộ phận quản trị hệ thống CNTT	Có ☐ Không ☐
Tổng số nhân sự quản trị hệ thống	
Có phân công nhân sự theo từng hệ thống (network, server, database,...)	Có ☐ Không ☐
Có nhân sự dự phòng cho vị trí quản trị hệ thống quan trọng	Có ☐ Không ☐
Số lượng nhân sự dự phòng	
Có danh sách liên hệ khẩn cấp	Có ☐ Không ☐
Có chương trình đào tạo định kỳ cho nhân sự CNTT	Có ☐ Không ☐
Tần suất đào tạo	Hàng năm
	2 năm/lần
	Không cố định

Đính kèm: Sơ đồ tổ chức bộ phận CNTT, phân công nhiệm vụ cụ thể

Danh sách các nhân viên chuyên môn về công nghệ thông tin quản lý, vận hành hệ thống GDCKTT:

STT	Họ và tên	Trình độ chuyên môn		Chứng chỉ chuyên môn (nếu có)	Vị trí công việc đảm nhận
		Cao đẳng/Đại học/Sau đại học	Chuyên ngành đào tạo		
1					
2					
.....					

Đính kèm: bằng tốt nghiệp, các chứng chỉ liên quan

5. Nội dung khác (nếu có):

Chúng tôi cam kết chịu trách nhiệm hoàn toàn về tính chính xác, trung thực những nội dung trên.

Người đại diện theo pháp luật

(Ký, ghi rõ họ tên hoặc chữ ký số nếu là biểu mẫu điện tử)

Phụ lục II

BÁO CÁO HOẠT ĐỘNG CUNG CẤP DỊCH VỤ TRỰC TUYẾN

(Ban hành kèm theo Thông tư số /2026/TT-BTC ngày tháng năm 2026 của Bộ trưởng Bộ Tài chính quy định giao dịch điện tử trên thị trường chứng khoán)

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập - Tự do - Hạnh phúc

... , ngày... tháng... năm ...

BÁO CÁO HOẠT ĐỘNG CUNG CẤP DỊCH VỤ TRỰC TUYẾN

(Tính từ thời điểm ngày 01/01 đến hết ngày 31/12 của năm báo cáo)

Kính gửi: Ủy ban Chứng khoán Nhà nước

I. Thông tin chung

Tên tổ chức cung cấp dịch vụ:

Năm báo cáo:

Người phụ trách hệ thống CNTT:

Email:

Điện thoại:

II. Thông tin báo cáo

1. Tình hình cung cấp dịch vụ trực tuyến

1.1. Các phương thức giao dịch trực tuyến (GDDT) tổ chức cung cấp:

Giao dịch qua Web trading	Có ☐ Không ☐
Giao dịch qua Mobile trading	Có ☐ Không ☐
Giao dịch qua API	Có ☐ Không ☐
Giao dịch qua tổng đài điện thoại	Có ☐ Không ☐
Số điện thoại nhận lệnh	
Phương thức khác	

1.2. Quy mô cung cấp dịch vụ:

Tổng số tài khoản	
Số tài khoản sử dụng giao dịch trực tuyến trong kỳ	
Tỷ lệ sử dụng giao dịch trực tuyến	
Tổng giá trị giao dịch trực tuyến	
Tổng số lệnh giao dịch trực tuyến	

Số lệnh giao dịch Web	
Số lệnh giao dịch Mobile	
Số lệnh giao dịch API	
Tỷ lệ lệnh qua Mobile	
Tỷ lệ lệnh qua API	
Số người dùng API	

2. Thông tin xác thực và truy vết giao dịch

2.1. Giải pháp xác thực giao dịch:

- Có tích hợp hệ thống eKYC: Có ☐ Không ☐

- Có đối chiếu dữ liệu sinh trắc học với CSDLQG về dân cư: Có ☐ Không ☐

a) Đối với giao dịch đặt lệnh:

Áp dụng xác thực khớp đúng thông tin sinh trắc học: Có ☐ Không ☐

Cung cấp trên ứng dụng:

Mobile App ☐ Web ☐ Desktop App ☐ Khác ☐

Đơn vị cung cấp giải pháp xác thực:

b) Đối với giao dịch rút, chuyển tiền ra khỏi tài khoản chứng khoán:

- Giao dịch dưới 10 triệu đồng:

Sinh trắc học ☐ SMS OTP ☐ Voice OTP ☐ Email OTP ☐

Soft OTP ☐ Token OTP ☐ FIDO ☐ Chữ ký số ☐

Xác thực hai kênh ☐ Khác:...

- Giao dịch từ 10 triệu đồng trở lên:

Xác thực khớp đúng thông tin sinh trắc học: Có ☐ Không ☐

c) Thống kê chi tiết:

STT	Giải pháp xác thực	Số tài khoản thực tế sử dụng trong năm	Số lệnh đặt
1	SMS OTP		
2	Voice OTP		
3	Email OTP		
5	Soft OTP		
6	Token OTP		
8	Xác thực khớp đúng thông tin sinh trắc học		
9	Xác thực khớp đúng thông tin sinh trắc học thiết bị		
10	FIDO		
11	Xác thực hai kênh		
12	Xác thực sử dụng chữ ký số		
13	Khác		

2.2. Lưu trữ thông tin truy cập giao dịch:

- Có thực hiện lưu trữ thông tin định danh thiết bị: Có ☐ Không ☐
- Thông tin lưu trữ:
 - + Đối với giao dịch qua web:
 - + Đối với giao dịch qua mobile app:
- Có lưu log xác thực giao dịch: Có ☐ Không ☐
- Có lưu log truy cập: Có ☐ Không ☐

3. Quy mô đầu tư trang bị hạ tầng phần cứng, phần mềm ứng dụng

3.1. Phần cứng

STT	Thiết bị	Số lượng	Ghi chú
...	Máy chủ		
	Router		
	Switch		
	Firewall		
	Thiết bị cân bằng tải		
	Hệ thống lưu trữ		(dung lượng)
	...		

3.2. Phần mềm

Địa chỉ website giao dịch	
Tên ứng dụng mobile	
Link App Store	
Link Google Play	
Đăng ký trên Android/iOS	Có ☐ Không ☐
Nhà cung cấp	
Công nghệ phát triển	(Java, .NET, Python, Node.js, PHP, Khác)
Hệ điều hành server	(Windows Server/Linux (Ubuntu/CentOS)/Unix/ Khác)
CSDL sử dụng	(Oracle/SQL Server/PostgreSQL/MySQL/Khác)

3.3. Triển khai API

Có cung cấp API giao dịch	Có ☐ Không ☐
Số lượng ứng dụng kết nối API	
Có sandbox cho API	Có ☐ Không ☐
Có quy trình phê duyệt kết nối API	Có ☐ Không ☐
Có kiểm soát thuật toán giao dịch	Có ☐ Không ☐
Có giới hạn truy cập API (rate limit)	Có ☐ Không ☐
Có giám sát lưu lượng API:	Có ☐ Không ☐
Có cảnh báo bất thường:	Có ☐ Không ☐

Số sự cố liên quan API	
Có cơ chế ngắt kết nối khẩn cấp API	Có ☐ Không ☐
Cơ chế xác thực API	API Key ☐ OAuth2 ☐ JWT ☐ Khác ☐
Có phân quyền truy cập API:	Có ☐ Không ☐
Có mã hóa kết nối	Có ☐ Không ☐
Có ghi log truy cập API:	Có ☐ Không ☐
Có khả năng truy vết giao dịch qua API:	Có ☐ Không ☐
Có quản lý version API:	Có ☐ Không ☐

Danh sách API:

STT	Tên API	Mục đích triển khai	Đối tác	Đối tượng sử dụng	Số lượng khách hàng sử dụng
1				+ Khách hàng cá nhân ☐ + Khách hàng tổ chức ☐ + Khác ☐	
2				+ Khách hàng cá nhân ☐ + Khách hàng tổ chức ☐ + Khác ☐	
..	...				

4. Khả năng đáp ứng của hệ thống GDCKTT

4.1. Công suất hệ thống (Lệnh/giây)

Năng lực thiết kế (khả năng tối đa theo thiết kế)	
Năng lực thực tế (mức tải cao nhất đã vận hành)	
Lệnh thị trường (lượng lệnh cao nhất phát sinh)	
Tỷ lệ sử dụng năng lực hệ thống	
Ngưỡng cảnh báo công suất	

4.2. Hiệu năng xử lý

STT	Nhóm chỉ tiêu	Chỉ tiêu	Giá trị
1	Thời gian phản hồi	Thời gian phản hồi trung bình của hệ thống	
2		Thời gian phản hồi tối đa (peak)	
3	Độ trễ giao dịch	Latency đặt lệnh (độ trễ từ khi lệnh được gửi đến hệ thống giao dịch đến khi được ghi nhận trong hệ thống xử lý lệnh)	
4		Latency phản hồi kết quả lệnh cho người dùng	
5	Độ ổn định giao dịch	Tỷ lệ lỗi giao dịch	
6		Tỷ lệ lệnh bị từ chối do lỗi hệ thống	

STT	Nhóm chỉ tiêu	Chỉ tiêu	Giá trị
7	Khả năng xử lý tải	Thời gian phản hồi khi hệ thống đạt tải cao (ví dụ >80% công suất)	
8	Giám sát vận hành	Có giám sát hiệu năng hệ thống theo thời gian thực	Có ☐ Không ☐
9		Có cơ chế cảnh báo khi hiệu năng suy giảm	Có ☐ Không ☐

4.3. Khả năng mở rộng

STT	Nhóm chỉ tiêu	Chỉ tiêu	Giá trị
1	Tự động mở rộng tài nguyên	Có cơ chế tự động mở rộng (auto scaling)	Có ☐ Không ☐
2		Hình thức mở rộng (scale out/in, scale up)	
3		Thời gian mở rộng tài nguyên	
4	Khả năng nâng cấp hệ thống	Có thể nâng cấp không gián đoạn (zero-downtime)	Có ☐ Không ☐
5		Có hỗ trợ rolling upgrade	Có ☐ Không ☐
6		Thời gian nâng cấp trung bình	...
7	Dự phòng tải cao	Có cơ chế phân tải (load balancing)	Có ☐ Không ☐
8		Có khả năng xử lý khi tải tăng đột biến	Có ☐ Không ☐
9		Ngưỡng tải tối đa có thể mở rộng thêm	

5. An toàn bảo mật

5.1 Bảo mật hệ thống

Có firewall bảo vệ hệ thống Có ☐ Không ☐

Có Web Application Firewall (WAF) Có ☐ Không ☐

Có hệ thống IDS/IPS Có ☐ Không ☐

Có giải pháp chống DDoS Có ☐ Không ☐

Tỷ lệ server đã cập nhật bản vá bảo mật (%)

- Quản lý log và giám sát hệ thống

Có hệ thống log tập trung Có ☐ Không ☐

Thời gian lưu log hệ thống

Có hệ thống SIEM Có ☐ Không ☐

Số rule phát hiện tấn công đang hoạt động

Số sự kiện an ninh được phát hiện trong năm

Có SOC giám sát hệ thống

Có ☐ Không ☐

Hình thức SOC

Nội bộ / Thuê ngoài

- Kiểm tra đánh giá bảo mật

Có thực hiện kiểm thử xâm nhập (Pentest) trong năm Có ☐ Không ☐

Số lần pentest trong năm:

Số lỗ hổng nghiêm trọng phát hiện:

Số lỗ hổng nghiêm trọng chưa khắc phục > 30 ngày:

Có kiểm tra cấu hình bảo mật định kỳ:

Có đánh giá bảo mật bởi bên thứ ba:

Đính kèm báo cáo penstest:

- Phần mềm

STT	Nhóm chỉ tiêu	Chỉ tiêu	Giá trị
1	Quản lý phát triển phần mềm	Có áp dụng quy trình phát triển an toàn (Secure SDLC)	Có ☐ Không ☐
2		Có kiểm tra mã nguồn (code review)	Có ☐ Không ☐
3		Có kiểm tra lỗ hổng (SAST/DAST)	Có ☐ Không ☐
4	Quản lý lỗ hổng & cập nhật	Có rà soát lỗ hổng định kỳ	Có ☐ Không ☐
5		Có cập nhật bản vá bảo mật	Có ☐ Không ☐
6		Thời gian xử lý lỗ hổng	...
7	Xác thực & phân quyền	Có cơ chế xác thực người dùng (MFA)	Có ☐ Không ☐
8		Có phân quyền truy cập theo vai trò	Có ☐ Không ☐
9		Có kiểm soát phiên đăng nhập (session)	Có ☐ Không ☐
10	Bảo vệ dữ liệu	Có mã hóa dữ liệu khi truyền (TLS/HTTPS)	Có ☐ Không ☐
11		Có mã hóa dữ liệu lưu trữ (encryption at rest)	Có ☐ Không ☐
12		Có che/mã hóa dữ liệu nhạy cảm	Có ☐ Không ☐

5.2 Bảo mật người dùng

STT	Nhóm chỉ tiêu	Chỉ tiêu	Giá trị
1	Xác thực người dùng	Có áp dụng xác thực đa yếu tố (MFA)	Có ☐ Không ☐
2		Phương thức xác thực	Password ☐ OTP ☐ Sinh trắc học ☐ Khác ☐
3	Quản lý mật khẩu	Có chính sách mật khẩu (độ dài, độ phức tạp)	Có ☐ Không ☐

4		Có yêu cầu thay đổi mật khẩu định kỳ	Có ☐ Không ☐
5		Có lưu mật khẩu dưới dạng mã hóa (hash)	Có ☐ Không ☐
6		Có giới hạn thời gian phiên (session timeout)	Có ☐ Không ☐
7	Quản lý phiên đăng nhập	Có tự động đăng xuất khi không hoạt động	Có ☐ Không ☐
8		Có kiểm soát đăng nhập đồng thời	Có ☐ Không ☐
9	Kiểm soát truy cập & thiết bị	Có ghi nhận thiết bị/IP đăng nhập	Có ☐ Không ☐
10		Có nhận diện thiết bị lạ	Có ☐ Không ☐
11		Có cảnh báo đăng nhập bất thường	Có ☐ Không ☐
12	Phòng chống gian lận	Có giới hạn số lần đăng nhập sai	Có ☐ Không ☐
13		Có cơ chế khóa tài khoản khi nghi ngờ rủi ro	Có ☐ Không ☐
14		Có phát hiện hành vi bất thường (fraud detection)	Có ☐ Không ☐
15	Thông báo và công khai thông tin	Có gửi thông báo khi đăng nhập/giao dịch	Có ☐ Không ☐
16		Có cho phép người dùng tra cứu lịch sử đăng nhập/giao dịch	Có ☐ Không ☐

5.3 Bảo mật dữ liệu

STT	Nhóm chỉ tiêu	Chỉ tiêu	Giá trị
1	Phân loại & quản lý dữ liệu	Có phân loại dữ liệu (công khai/nội bộ/mật...)	Có ☐ Không ☐
2		Có quy định quản lý dữ liệu nhạy cảm	Có ☐ Không ☐
3	Mã hóa dữ liệu	Có mã hóa dữ liệu khi truyền (TLS/HTTPS)	Có ☐ Không ☐
4		Có mã hóa dữ liệu lưu trữ (encryption at rest)	Có ☐ Không ☐
5	Kiểm soát truy cập dữ liệu	Có phân quyền truy cập dữ liệu theo vai trò	Có ☐ Không ☐
6		Có kiểm soát truy cập dữ liệu nhạy cảm	Có ☐ Không ☐

7		Có ghi log truy cập dữ liệu	Có ☐ Không ☐
8	Bảo vệ dữ liệu người dùng	Có che/mã hóa dữ liệu nhạy cảm (masking/tokenization)	Có ☐ Không ☐
9		Có ẩn thông tin khi hiển thị (ví dụ: ****)	Có ☐ Không ☐

6. Dự phòng sự cố

- Dự phòng hệ thống, dữ liệu

STT	Nhóm chỉ tiêu	Chỉ tiêu	Giá trị	Ghi chú
1	Dự phòng hệ thống	Có hệ thống dự phòng (DR site)	Có ☐ Không ☐	
2		Mô hình dự phòng	Active-Active ☐ Active-Passive ☐	
3	Dự phòng dữ liệu	Có sao lưu dữ liệu	Có ☐ Không ☐	Tự động ☐ Thủ công ☐
4		Tần suất sao lưu	...	
5		Có đồng bộ dữ liệu thời gian thực (replication)	Có ☐ Không ☐	
6	Khả năng khôi phục	RTO (thời gian khôi phục)	...	
7		RPO (mất dữ liệu tối đa cho phép)	...	
8		Có kiểm tra khôi phục định kỳ	Có ☐ Không ☐	

- Giải pháp quản lý, ứng phó sự cố bảo mật

STT	Nhóm chỉ tiêu	Chỉ tiêu	Giá trị
1	Quy trình & tổ chức	Có quy trình xử lý sự cố (Incident Response)	Có ☐ Không ☐
2		Có kịch bản ứng phó cho từng loại sự cố (tấn công, lỗi hệ thống...)	Có ☐ Không ☐
3		Có phân công đầu mối xử lý sự cố	Có ☐ Không ☐
4	Phát hiện & cảnh báo	Có hệ thống giám sát an toàn thông tin	Có ☐ Không ☐
5		Có cảnh báo sự cố theo thời gian thực	Có ☐ Không ☐
6	Xử lý sự cố	Có cơ chế cô lập hệ thống khi xảy ra sự cố	Có ☐ Không ☐
7		Có cơ chế ngắt dịch vụ khẩn cấp	Có ☐ Không ☐
8	Báo cáo & khắc	Có ghi nhận và lưu vết sự cố	Có ☐ Không ☐

STT	Nhóm chỉ tiêu	Chỉ tiêu	Giá trị
9	phục	Có quy trình báo cáo sự cố	Có ☐ Không ☐
10		Có hệ thống quản lý log tập trung phục vụ điều tra sự cố	Có ☐ Không ☐
11		Có thực hiện khắc phục sau sự cố	Có ☐ Không ☐

- Diễn tập:

STT	Nội dung	
1	Có thực hiện diễn tập xử lý sự cố	Có ☐ Không ☐
2	Tần suất diễn tập	
3	Có diễn tập chuyển đổi sang hệ thống DR	Có ☐ Không ☐
4	Có kiểm thử failover thực tế	Có ☐ Không ☐
5	Có đánh giá, rút kinh nghiệm sau diễn tập	Có ☐ Không ☐

7. Năng lực quản trị và vận hành CNTT

7.1. Nhân sự CNTT

Có bộ phận CNTT độc lập

Tổng số nhân sự CNTT:

Có phân công rõ trách nhiệm (phát triển phần mềm/vận hành hệ thống/an toàn thông tin) Có ☐ Không ☐

Có bộ phận chuyên trách an toàn thông tin (ATTT): Có ☐ Không ☐

Số nhân sự chuyên trách ATTT:

Có đội ứng cứu sự cố CNTT: Có ☐ Không ☐

Tần suất đào tạo:

7.2. Quản trị vận hành

Có quy trình vận hành hàng ngày: Có ☐ Không ☐

Có quản lý thay đổi hệ thống: Có ☐ Không ☐

Có cập nhật phần mềm/vá lỗi thường xuyên: Có ☐ Không ☐

Có theo dõi, giám sát 24/7: Có ☐ Không ☐

Có cáo cáo tổng hợp hàng ngày: Có ☐ Không ☐

8. Sự cố an toàn thông tin:

Số sự cố an ninh mạng xảy ra trong năm:

Số sự cố hệ thống giao dịch:

Số sự cố tấn công mạng:

Số sự cố chiếm quyền tài khoản khách hàng:

Số sự cố nghiêm trọng:

Tổng thời gian gián đoạn hệ thống:

9. Thay đổi hệ thống giao dịch

Số lần nâng cấp hệ thống trong năm:

Số lần thay đổi lớn (major release):

Có kiểm thử trước khi triển khai: Có ☐ Không ☐

10. Tuân thủ pháp luật và tiêu chuẩn

10.1. Tiêu chuẩn ATTT

- Tiêu chuẩn ATTT áp dụng (ISO 27001, theo quy định về ATTT cấp độ):
- Phạm vi áp dụng (hệ thống giao dịch trực tuyến, trung tâm dữ liệu,...):
- Tình trạng chứng nhận (đã chứng nhận/đang triển khai):
- Thời hạn chứng chỉ (ngày cấp, ngày hết hạn):
- Đơn vị đánh giá:

10.2. Quy định lưu trữ dữ liệu

STT	Loại dữ liệu	Thời gian lưu trữ	Lưu trữ (Online/Offline)	Vị trí (DC/DR/Cloud)	Sao lưu	Tần suất	Mã hóa	Kiểm tra khôi phục
1	Dữ liệu giao dịch							
2	Log hệ thống							
3	Dữ liệu khách hàng							
4	Dữ liệu cấu hình hệ thống							

10.3. Quy định bảo vệ dữ liệu cá nhân

STT	Nội dung	Mô tả/Chỉ tiêu	Thực tế triển khai tại đơn vị
1	Thu thập dữ liệu cá nhân	Loại dữ liệu thu thập	Định danh ☐ Liên hệ ☐ Sinh trắc học ☐ Khác ☐
2		Nguồn thu thập (khách hàng cung cấp/hệ thống ghi nhận)	
3		Có thông báo/đồng ý của khách	Có ☐ Không ☐

		hàng	
4	Mục đích sử dụng	Mục đích xử lý dữ liệu	Giao dịch ☐ Xác thực ☐ Pháp lý ☐ Khác ☐
5		Có sử dụng đúng mục đích đã thông báo	Có ☐ Không ☐
6	Biện pháp bảo vệ dữ liệu	Có mã hóa dữ liệu	Có ☐ Không ☐
7		Có phân quyền truy cập dữ liệu	Có ☐ Không ☐
8		Có che/mã hóa dữ liệu nhạy cảm	Có ☐ Không ☐
9		Có kiểm soát truy cập nội bộ	Có ☐ Không ☐
10	Quyền của khách hàng	Cho phép truy cập/xem dữ liệu	Có ☐ Không ☐
11		Cho phép chỉnh sửa/cập nhật	Có ☐ Không ☐
12		Cho phép yêu cầu xóa dữ liệu	Có ☐ Không ☐
13	Chia sẻ và cung cấp dữ liệu	Có chia sẻ dữ liệu cho bên thứ ba	Có ☐ Không ☐
14		Có kiểm soát/điều kiện khi chia sẻ	Có ☐ Không ☐
15	Xử lý sự cố rò rỉ dữ liệu	Có quy trình xử lý sự cố	Có ☐ Không ☐
16		Có phát hiện và cảnh báo rò rỉ	Có ☐ Không ☐
17		Có thông báo cho cơ quan quản lý	Có ☐ Không ☐
18		Có thông báo cho khách hàng bị ảnh hưởng	Có ☐ Không ☐
19	Lưu trữ & vòng đời dữ liệu	Có quy định thời gian lưu trữ dữ liệu cá nhân	Có ☐ Không ☐
20		Có cơ chế xóa/hủy dữ liệu khi hết mục đích	Có ☐ Không ☐

11. Nội dung khác (nếu có):

12. Các khó khăn vướng mắc trong quá trình cung cấp dịch vụ (về pháp lý, về đầu tư công nghệ,...):

13. Kiến nghị, đề xuất (nếu có):

Người đại diện theo pháp luật
(Ký, ghi rõ họ tên hoặc chữ ký số
nếu là biểu mẫu điện tử)

Phụ lục III

BÁO CÁO TRIỂN KHAI DỊCH VỤ API

(Ban hành kèm theo Thông tư số /2026/TT-BTC ngày tháng năm 2026 của Bộ trưởng Bộ Tài chính quy định giao dịch điện tử trên thị trường chứng khoán)

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập - Tự do - Hạnh phúc

... , ngày... tháng... năm ...

BÁO CÁO TRIỂN KHAI DỊCH VỤ API

Kính gửi: Ủy ban Chứng khoán Nhà nước

I. Thông tin chung

Tên tổ chức cung cấp dịch vụ:

Địa chỉ trụ sở chính:

Ngày lập báo cáo:

Người lập báo cáo:

Điện thoại:

Email:

II. Thông tin báo cáo

1. Thông tin dịch vụ API

Tên dịch vụ API:

Loại API:

(Partner API / Internal API/khác)

Mục đích triển khai

- ☐ đặt lệnh giao dịch
- ☐ truy vấn dữ liệu
- ☐ quản lý tài khoản
- ☐ dữ liệu thị trường
- ☐ giao dịch thuật toán
- ☐ khác (mô tả:...)

Phạm vi khách hàng

- ☐ cá nhân
- ☐ tổ chức
- ☐ fintech
- ☐ đối tác

- Chuẩn giao thức API ☐ REST
☐ FIX
☐ WebSocket
☐ GraphQL
 Khác
- Môi trường cung cấp ☐ Sandbox
☐ Test
☐ Production

Ngày bắt đầu thử nghiệm

Ngày chính thức triển khai

Đính kèm tài liệu kỹ thuật mô tả chi tiết về API

2. Thông tin đối tác tích hợp API

- Tên đối tác:
- Loại đối tác: Fintech
☐ Công ty công nghệ
☐ Công ty quản lý quỹ
☐ Tổ chức tài chính
☐ Khác (mô tả...)
- Hình thức kết nối: ☐ Internet
☐ VPN
☐ Private Line
- Có hợp đồng dịch vụ: Có ☐ Không ☐
- Có đánh giá an toàn thông tin đối tác: Có ☐ Không ☐
- Có kiểm tra bảo mật định kỳ: Có ☐ Không ☐
- Có giới hạn quyền API theo đối tác: Có ☐ Không ☐
- Đính kèm tài liệu đánh giá đối tác (Upload file)

3. Chức năng API cung cấp

Chức năng API	Có cung cấp	Số endpoint	Xác thực áp dụng	Kiểm soát truy cập
Đặt lệnh giao dịch	Có ☐ Không ☐			Có ☐ Không ☐
Truy vấn trạng thái lệnh	Có ☐ Không ☐			Có ☐ Không ☐
Quản lý tài khoản	Có ☐ Không ☐			Có ☐ Không ☐
Truy vấn danh mục	Có ☐ Không ☐			Có ☐ Không ☐
Dữ liệu thị trường	Có ☐ Không ☐			Có ☐ Không ☐
Chức năng khác	Có ☐ Không ☐			Có ☐ Không ☐

4. An toàn bảo mật API

	☐ API Key
	☐ OAuth2
Cơ chế xác thực API	☐ JWT
	☐ Mutual TLS
	☐ Khác
Có mã hóa TLS	Có ☐ Không ☐
Có IP whitelist	Có ☐ Không ☐
Có rate limit	Có ☐ Không ☐
Có giám sát API realtime	Có ☐ Không ☐
Có ghi log request	Có ☐ Không ☐
Thời gian lưu log (ngày):	
Tiêu chuẩn bảo mật áp dụng:	

5. Quản lý rủi ro API:

Có quy trình quản lý API:	Có ☐ Không ☐
Có kiểm soát giao dịch thuật toán:	Có ☐ Không ☐
Có cơ chế ngắt API khẩn cấp:	Có ☐ Không ☐
Số sự cố API trong kỳ:	
Số sự cố an toàn thông tin:	
Số lần phát hiện truy cập bất thường:	
Có kiểm thử bảo mật định kỳ:	Có ☐ Không ☐

Đính kèm: Tài liệu kỹ thuật, Tài liệu quản lý rủi ro, Biện pháp bảo vệ thông tin khách hàng, Chính sách kiểm soát truy cập, tài liệu khác...

6. Nội dung khác (nếu có):

Người đại diện theo pháp luật
*(Ký, ghi rõ họ tên hoặc chữ ký số
 nếu là biểu mẫu điện tử)*

Phụ lục IV

BÁO CÁO QUẢN LÝ, VẬN HÀNH HỆ THỐNG GIAO DỊCH CHỨNG KHOÁN CỦA SỞ GIAO DỊCH CHỨNG KHOÁN

(Ban hành kèm theo Thông tư số /2026/TT-BTC ngày tháng năm 2026 của Bộ trưởng Bộ Tài chính quy định giao dịch điện tử trên thị trường chứng khoán)

BỘ TÀI CHÍNH
SỞ GIAO DỊCH CHỨNG KHOÁN VIỆT NAM

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

Số: , ngày tháng năm

BÁO CÁO QUẢN LÝ, VẬN HÀNH HỆ THỐNG GIAO DỊCH CHỨNG KHOÁN NĂM

(Tính từ thời điểm ngày 01/01 đến hết ngày 31/12 của năm báo cáo)

Kính gửi: Ủy ban Chứng khoán Nhà nước

1. Các văn bản quy định liên quan đến hoạt động cung cấp dịch vụ giao dịch do Sở GDCK Việt Nam và công ty con ban hành mới trong năm

STT	Tên văn bản	Số văn bản	Ngày ban hành
1			
2			
...			

Đính kèm các quy trình ban hành mới trong năm báo cáo (nếu có).

3. Thành viên giao dịch

Biểu 1: Thống kê thành viên giao dịch

STT	Số thành viên đầu kỳ	Số thành viên được chấp thuận trong năm	Số thành viên bị hủy bỏ tư cách	Số thành viên cuối kỳ

Biểu 2: Hoạt động chấp thuận tư cách thành viên

STT	Tên Thành viên	Ngày chấp thuận

Biểu 3: Hoạt động hủy bỏ tư cách thành viên

STT	Tên Thành viên	Ngày hủy bỏ

Biểu 4: Danh sách thành viên hiện tại

STT	Tên Thành viên	Ghi chú

4. Thành viên kết nối đến các công ty con:**4.1. Danh sách thành viên kết nối đến Sở GDCK Tp. Hồ Chí Minh**

STT	Tên Thành viên	Ghi chú

4.2. Danh sách thành viên kết nối đến Sở GDCK Hà Nội

STT	Tên Thành viên	Ghi chú

5. Các dịch vụ giao dịch điện tử cung cấp cho thành viên:

STT	Tên dịch vụ	Mô tả dịch vụ	Ngày triển khai	Số thành viên sử dụng

6. Thống kê sự cố giao dịch trong năm:

Tổng số sự cố hệ thống giao dịch trong năm:

Tổng thời gian gián đoạn giao dịch (phút):

Số ngày giao dịch bị ảnh hưởng:

Số sự cố mức nghiêm trọng:

Số sự cố mức trung bình:

Số sự cố mức nhẹ:

Có sự cố phải tạm ngừng giao dịch toàn thị trường:

Hệ thống bị ảnh hưởng:

- Lỗi phần mềm
- Lỗi cấu hình
- Lỗi hạ tầng máy chủ
- Lỗi mạng
- Quá tải hệ thống
- Lỗi tích hợp hệ thống
- Lỗi thao tác vận hành
- Tấn công mạng
- Nguyên nhân bên thứ ba

Khác:

Phạm vi ảnh hưởng:

- Toàn thị trường
- Một nhóm thành viên
- Một số dịch vụ
- Không ảnh hưởng giao dịch

7. Biện pháp khắc phục sự cố:

8. Nội dung khác (nếu có):

Thông tin của người lập báo cáo:

Họ và tên:.....

Điện thoại:Email:.....

TỔNG GIÁM ĐỐC

*(Ký tên, ghi rõ họ tên hoặc chữ ký số
nếu là biểu mẫu điện tử)*

Phụ lục V

**BÁO CÁO QUẢN LÝ, VẬN HÀNH HỆ THỐNG CUNG CẤP DỊCH VỤ CỦA
TỔNG CÔNG TY LƯU KÝ VÀ BÙ TRỪ CHỨNG KHOÁN VIỆT NAM**

*(Ban hành kèm theo Thông tư số /2026/TT-BTC ngày tháng năm 2026 của
Bộ trưởng Bộ Tài chính quy định giao dịch điện tử trên thị trường chứng khoán)*

**BỘ TÀI CHÍNH
TỔNG CÔNG TY LƯU KÝ VÀ BÙ TRỪ
CHỨNG KHOÁN VIỆT NAM**

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

Số: , ngày tháng năm

**BÁO CÁO QUẢN LÝ, VẬN HÀNH HỆ THỐNG CUNG CẤP DỊCH VỤ
NĂM**

(Tính từ thời điểm ngày 01/01 đến hết ngày 31/12 của năm báo cáo)

Kính gửi: Ủy ban Chứng khoán Nhà nước

**1. Các văn bản quy định liên quan đến hoạt động cung cấp dịch vụ trực
tuyến ban hành trong năm**

STT	Tên văn bản	Số văn bản	Ngày ban hành
1			
2			
...			

Đính kèm các quy trình ban hành mới trong năm báo cáo (nếu có).

2. Hoạt động cung cấp dịch vụ trực tuyến

Các dịch vụ trực tuyến cung cấp cho thành viên

STT	Tên dịch vụ	Số lượng thành viên sử dụng dịch vụ
1		
2		
...		

3. Nội dung khác (nếu có):

Thông tin của người lập báo cáo:

Họ và tên:

Điện thoại: Email:

TỔNG GIÁM ĐỐC

*(Ký tên, ghi rõ họ tên hoặc chữ ký số
nếu là biểu mẫu điện tử)*

Phụ lục VI

BÁO CÁO SỰ CỐ HỆ THỐNG GIAO DỊCH TRỰC TUYẾN

(Ban hành kèm theo Thông tư số /2026/TT-BTC ngày tháng năm 2026 của Bộ trưởng Bộ Tài chính quy định giao dịch điện tử trên thị trường chứng khoán)

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập - Tự do - Hạnh phúc

...., ngày... tháng... năm ...

BÁO CÁO SỰ CỐ HỆ THỐNG GIAO DỊCH TRỰC TUYẾN

Kính gửi: Ủy ban Chứng khoán Nhà nước

Tổ chức cung cấp dịch vụ:

Thông tin người phụ trách GDCKTT:

Họ và tên:

Địa chỉ Email:Điện thoại:

1. Thông tin sự cố:

Ngày xảy ra sự cố:

Thời điểm bắt đầu:

Thời điểm khắc phục:

Tổng thời gian gián đoạn (phút):

Hệ thống bị ảnh hưởng:

- Hệ thống giao dịch trực tuyến Web
- Mobile trading
- API giao dịch
- FIX Gateway
- Hệ thống quản lý tài khoản
- Hệ thống xác thực
- Hạ tầng mạng
- Hạ tầng máy chủ
- Khác

Dịch vụ giao dịch bị ảnh hưởng:

- Đăng nhập
- Đặt lệnh
- Sửa/hủy lệnh
- Tra cứu tài khoản

- Nộp/rút tiền
- Dữ liệu thị trường

2. Phân loại sự cố:

- Loại sự cố:
- Lỗi phần mềm
 - Lỗi cấu hình hệ thống
 - Lỗi hạ tầng máy chủ
 - Lỗi mạng
 - Quá tải hệ thống
 - Lỗi tích hợp hệ thống
 - Lỗi thao tác vận hành
 - Tấn công mạng
 - Lỗi từ bên thứ ba

Mức độ sự cố: Nghiêm trọng/Cao/trung bình/thấp

- Phạm vi ảnh hưởng:
- Toàn bộ khách hàng
 - Một nhóm khách hàng
 - Một phần dịch vụ
 - Nội bộ hệ thống

3. Mô tả sự cố:

Đính kèm mô tả chi tiết về sự cố

4. Đánh giá ảnh hưởng:

Số lượng khách hàng bị ảnh hưởng:

Số lượng lệnh bị ảnh hưởng:

Có phát sinh thiệt hại tài chính: Có ☐ Không ☐

Giá trị thiệt hại (nếu có):

Có ảnh hưởng thị trường: Có ☐ Không ☐

Mô tả chi tiết ảnh hưởng:

5. Biện pháp xử lý:

Biện pháp khắc phục sự cố:

Thời gian khắc phục hoàn toàn:

Biện pháp phòng ngừa tái diễn:

Thay đổi hệ thống sau sự cố: Có ☐ Không ☐

6. Kết quả khắc phục:

- Trạng thái hệ thống sau khắc phục:
- Hoạt động bình thường
 - Hoạt động hạn chế
 - Tiếp tục theo dõi

Có tái phát sự cố: Có ☐ Không ☐

Thời điểm hệ thống hoạt động bình thường

7. Nội dung khác (nếu có):

TỔNG GIÁM ĐỐC

(Ký, ghi rõ họ tên

hoặc chữ ký số nếu là biểu mẫu điện tử)

Phụ lục VII**BÁO CÁO SỰ CỐ HỆ THỐNG GIAO DỊCH CỦA CÁC SỞ GIAO DỊCH
CHỨNG KHOÁN, TỔNG CÔNG TY LƯU KÝ VÀ BÙ TRỪ
CHỨNG KHOÁN VIỆT NAM**

*(Ban hành kèm theo Thông tư số /2026/TT-BTC ngày tháng năm 2026 của
Bộ trưởng Bộ Tài chính quy định giao dịch điện tử trên thị trường chứng khoán)*

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập - Tự do - Hạnh phúc

...., ngày... tháng... năm ...

BÁO CÁO SỰ CỐ HỆ THỐNG GIAO DỊCH

Kính gửi: Ủy ban Chứng khoán Nhà nước

Sở GDCK...../Tổng công ty Lưu ký và Bù trừ chứng khoán Việt Nam báo cáo sự cố hệ thống giao dịch như sau:

1. Thông tin sự cố:

Thời gian phát sinh sự cố

Thời gian phát hiện sự cố

Thời gian khắc phục

Tổng thời gian gián đoạn (phút)

Trạng thái sự cố

- Đã khắc phục ☐
- Đang xử lý ☐
- Đang theo dõi ☐

2. Hệ thống bị ảnh hưởng

Hệ thống bị ảnh hưởng

- Hệ thống giao dịch ☐
- Hệ thống nhận lệnh ☐
- Hệ thống bù trừ thanh toán ☐
- Hệ thống quản lý thành viên ☐
- Hạ tầng mạng ☐
- Hạ tầng máy chủ ☐
- Khác ☐

Dịch vụ bị ảnh hưởng

- Nhận lệnh ☐
- Khớp lệnh ☐

- Sửa/hủy lệnh ☐
- Kết nối thành viên ☐
- API / FIX ☐

Phạm vi ảnh hưởng

- Toàn thị trường ☐
- Một nhóm thành viên ☐
- Một số dịch vụ ☐
- Không ảnh hưởng giao dịch ☐

3. Mô tả sơ bộ sự cố:

Đính kèm nội dung mô tả chi tiết sự cố.

4. Nguyên nhân sự cố:

Nguyên nhân chính

- Lỗi phần mềm ☐
- Lỗi cấu hình ☐
- Lỗi hạ tầng máy chủ ☐
- Lỗi mạng ☐
- Quá tải hệ thống ☐
- Lỗi tích hợp hệ thống ☐
- Lỗi thao tác vận hành ☐
- Tấn công mạng ☐
- Lỗi bên thứ ba ☐

Nguyên nhân chi tiết:

5. Đánh giá rủi ro và ảnh hưởng

Mức độ sự cố

- Nghiêm trọng (dừng giao dịch) ☐
- Cao (không nhận lệnh) ☐
- Trung bình (chậm/gián đoạn) ☐
- Thấp (ảnh hưởng nhỏ) ☐

Có ảnh hưởng đến giao dịch thị trường

Có ☐ Không ☐

Số lượng thành viên bị ảnh hưởng

Số lượng lệnh bị ảnh hưởng

Có ảnh hưởng hệ thống khác

Có ☐ Không ☐

Mô tả ảnh hưởng

6. Tình hình thiệt hại

Có thiệt hại tài chính

Có ☐ Không ☐

Giá trị thiệt hại ước tính

Thiệt hại hệ thống

Thiệt hại khác

7. Biện pháp khắc phục

Biện pháp xử lý sự cố:

Biện pháp ngăn chặn tái diễn:

Có thay đổi hệ thống sau sự cố: Có ☐ Không ☐

8. Kết quả khắc phục

Thời điểm hệ thống hoạt động bình thường

Trạng thái hệ thống sau khắc phục

Có tái phát sự cố: Có ☐ Không ☐

9. Nội dung khác (nếu có):

Thông tin người phụ trách (kỹ thuật) hệ thống giao dịch:

Họ và tên:

Địa chỉ Email:

Điện thoại:

TỔNG GIÁM ĐỐC

*(Ký, ghi rõ họ tên hoặc chữ ký số
nếu là biểu mẫu điện tử)*

(Ban hành kèm theo Thông tư số /2026/TT-BTC ngày tháng năm 2026 của Bộ trưởng Bộ Tài chính quy định giao dịch điện tử trên thị trường chứng khoán)

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Số:

....., ngày... tháng... năm ...

Kính gửi: Ủy ban Chứng khoán Nhà nước

Công ty xin báo cáo các thay đổi liên quan đến hệ thống giao dịch trực tuyến của công ty như sau:

1. Thay đổi hệ thống Core giao dịch trực tuyến (khi có thay đổi):

Có thay đổi hệ thống Core Có ☐ Không ☐

Mô hình kiến trúc hệ thống Core: đính kèm mô hình chi tiết

Thuyết minh mô hình hệ thống, nội dung thay đổi: đính kèm thuyết minh chi tiết

Thay đổi máy chủ Có ☐ Không ☐

Thay đổi thiết bị mang Có ☐ Không ☐

Thay đổi đường truyền Có ☐ Không ☐

Thay đổi giải pháp bảo mật Có ☐ Không ☐

Thay đổi phần mềm hệ thống Có ☐ Không ☐

Thay đổi giải pháp sao lưu dữ liệu Có ☐ Không ☐

Thay đổi giải pháp lưu trữ dữ liệu Có ☐ Không ☐

Thay đổi hệ thống dự phòng Có ☐ Không ☐

Thay đổi giải pháp kiểm soát rủi ro hệ thống Có ☐ Không ☐

Thời gian vận hành chính thức sau thay đổi Date

2. Thay đổi website hoặc tên phần mềm cung cấp dịch vụ GDTT (khi có thay đổi):

Có thay đổi website / phần mềm giao dịch Có ☐ Không ☐

Địa chỉ website giao dịch

Tên phần mềm giao dịch

Phần mềm đã đăng ký trên kho ứng dụng Có ☐ Không ☐

Tên kho ứng dụng

• App Store ☐

• Google Play ☐

• Khác ☐

Tên ứng dụng trên kho

Phiên bản phần mềm

3. Nhân sự quản lý hệ thống GDDT (khi có thay đổi):

STT	Họ và tên	Vị trí công việc đảm nhận	Thay đổi (thêm mới, nghỉ việc)	Thời gian thay đổi

4. Địa điểm đặt hệ thống (khi có thay đổi):

Mô tả địa điểm đặt hệ thống giao dịch trực tuyến.

5. Nội dung thay đổi khác (nếu có):.....

Thông tin của người lập báo cáo:

Họ và tên:.....

Điện thoại di động:Email:.....

TỔNG GIÁM ĐỐC

(Ký, ghi rõ họ tên hoặc chữ ký số nếu là biểu mẫu điện tử)