Ký bởi: CỤC THUẾ
Cơ quan:
Thời gian ký: 27/08/2026 10:37:00+07:00

BỘ TÀI CHÍNH
CỤC THUẾ

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

Số: 1225/QĐ-CT

Hà Nội, ngày 26 tháng 8 năm 2026

QUYẾT ĐỊNH

Ban hành Quy chế An toàn thông tin cơ quan thuế

CỤC TRƯỞNG CỤC THUẾ

Căn cứ Luật Quản lý thuế ngày 10 tháng 12 năm 2025;

Căn cứ Luật An ninh mạng ngày 10 tháng 12 năm 2025;

Căn cứ Luật Bảo vệ bí mật nhà nước ngày 10 tháng 12 năm 2025;

Căn cứ Luật Bảo vệ dữ liệu cá nhân ngày 26 tháng 6 năm 2025;

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

Căn cứ Nghị định số 142/2016/NĐ-CP ngày 14/10/2016 của Chính phủ về ngăn chặn xung đột thông tin trên mạng;

Căn cứ Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ về việc quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Nghị định số 356/2025/NĐ-CP ngày 31/12/2025 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 252/2026/NĐ-CP ngày 30/6/2026 của Chính phủ quy định chi tiết một số điều và biện pháp để tổ chức thi hành Luật Quản lý thuế;

Căn cứ Quyết định số 381/QĐ-BTC ngày 26/02/2025 của Bộ trưởng Bộ Tài chính quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Cục Thuế; Quyết định số 1892/QĐ-BTC ngày 30/05/2025 và Quyết định số 2229/QĐ-BTC ngày 30/06/2025 của Bộ trưởng Bộ Tài chính sửa đổi, bổ sung Quyết định số 381/QĐ-BTC ngày 26/02/2025 của Bộ trưởng Bộ Tài chính quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Cục Thuế;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ ban hành Quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng Quốc gia;

Căn cứ Quyết định số 2405/QĐ-BTC ngày 08/7/2025 của Bộ trưởng Bộ Tài chính Ban hành Quy chế An toàn thông tin mạng và An toàn thông tin Bộ Tài chính;

Theo đề nghị của Trưởng Ban Công nghệ, chuyển đổi số và tự động hóa.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế An toàn thông tin cơ quan thuế.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký và thay thế Quyết định số 1731/QĐ-TCT ngày 08/11/2024 của Tổng cục trưởng Tổng cục Thuế về việc ban hành Quy chế An toàn thông tin mạng và An toàn thông tin ngành Thuế.

Điều 3. Trưởng Ban Công nghệ, chuyển đổi số và tự động hoá, Chánh Văn phòng, Trưởng Ban Tổ chức cán bộ, Trưởng Ban Quản lý tuân thủ và hỗ trợ người nộp thuế, Thủ trưởng các Ban/đơn vị thuộc Cơ quan Cục Thuế, Trưởng Thuế tỉnh, thành phố, các đơn vị có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Các đ/c P.CTrg (để p/h);
- Cục CNTT;
- Lưu: VT, CĐS.

CỤC TRƯỞNG

BỘ TÀI CHÍNH TỔNG CỤC THUẾ

Mai Xuân Thành

BỘ TÀI CHÍNH
CỤC THUẾ

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

QUY CHẾ
An toàn thông tin cơ quan thuế

(Kèm theo Quyết định số 1225/QĐ-CT ngày 26 tháng 8 năm 2026 của Cục Thuế)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh, đối tượng áp dụng

1. Quy chế này quy định về công tác an toàn thông tin tại các cơ quan thuế.

2. Quy chế này áp dụng với:

a) Công chức, viên chức, người lao động thuộc cơ quan thuế các cấp và các cơ quan, tổ chức, cá nhân bên ngoài tham gia xây dựng, phát triển, sử dụng, quản trị và vận hành an toàn thông tin cơ quan thuế hoặc có liên quan đến việc xử lý, truyền nhận hoặc bảo vệ thông tin Cục Thuế.

b) Các hệ thống, ứng dụng, dịch vụ công nghệ thông tin và vật lý được cơ quan thuế triển khai.

Điều 2. Giải thích từ ngữ và từ viết tắt

1. Giải thích từ ngữ:

a) An toàn thông tin cơ quan thuế được thực hiện trên các nhóm đối tượng sau: An ninh Hệ thống thông tin; An ninh dữ liệu; An ninh vật lý; An ninh con người.

b) Thiết bị xử lý thông tin là thiết bị dùng để tạo lập, xử lý, lưu trữ, truyền đưa thông tin dưới dạng điện tử (máy tính, máy in, điện thoại thông minh, thiết bị mạng, thiết bị an toàn thông tin, camera giám sát và các thiết bị tương tự khác).

c) Hệ thống thông tin là tập hợp phần cứng, phần mềm và dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên không gian mạng.

d) Người dùng là công chức, viên chức, người lao động tại các đơn vị thuộc cơ quan thuế, cá nhân bên ngoài tham gia xây dựng, phát triển, sử dụng, quản trị và vận hành hệ thống thông tin cơ quan thuế hoặc có sử dụng các dịch vụ do cơ quan thuế cung cấp, có kết nối trao đổi thông tin với cơ quan thuế.

đ) Chủ quản hệ thống thông tin là Cục Thuế hoặc cấp có thẩm quyền phê duyệt thuê dịch vụ công nghệ thông tin, quyết định đầu tư dự án xây dựng, thiết

lập, nâng cấp, mở rộng hệ thống thông tin theo phân cấp. Trường hợp không xác định được cấp có thẩm quyền phê duyệt dịch vụ công nghệ thông tin, quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin, chủ quản hệ thống thông tin là đơn vị có thẩm quyền quản lý trực tiếp hệ thống thông tin.

e) Đơn vị vận hành hệ thống thông tin Cục Thuế:

- Ban CĐS là đơn vị được giao vận hành hệ thống thông tin do Cục Thuế là chủ quản hệ thống thông tin.

- Văn phòng Cục Thuế là đơn vị được giao vận hành hệ thống camera giám sát do Cục Thuế làm chủ quản hệ thống thông tin.

- Thuế tỉnh, thành phố là đơn vị vận hành hệ thống thông tin:

+ Hệ thống mạng nội bộ triển khai tại cơ quan Thuế tỉnh, thành phố.

+ Hệ thống thông tin do cơ quan Thuế tỉnh, thành phố tự triển khai.

+ Hệ thống thông tin khác do Cục Thuế phân cấp, uỷ quyền.

- Thuế cơ sở là đơn vị vận hành hệ thống thông tin:

+ Hệ thống mạng nội bộ triển khai tại cơ quan Thuế cơ sở.

+ Hệ thống thông tin do cơ quan Thuế cơ sở tự triển khai.

+ Hệ thống thông tin khác do Thuế tỉnh, thành phố phân cấp, uỷ quyền.

- Đơn vị cung cấp dịch vụ thực hiện vai trò đơn vị vận hành hệ thống thông tin đang trong thời gian thuê dịch vụ công nghệ thông tin.

g) Đơn vị chuyên trách an toàn hệ thống thông tin:

- Ban CĐS đảm nhận vai trò đơn vị chuyên trách an toàn hệ thống thông tin tại Cục Thuế.

- Bộ phận chuyên trách về an toàn hệ thống thông tin tại Thuế tỉnh, thành phố do Thuế tỉnh, thành phố thành lập hoặc phân công để thực thi nhiệm vụ bảo đảm an toàn thông tin và ứng cứu sự cố an toàn thông tin mạng.

h) Bộ phận công nghệ thông tin (Bộ phận CNTT):

- Tại cơ quan Cục Thuế là Ban Công nghệ, chuyển đổi số và tự động hóa.

- Tại Thuế tỉnh, thành phố là phòng Quản lý dữ liệu và quản trị rủi ro.

- Tại Thuế cơ sở là bộ phận được phân công làm công tác công nghệ thông tin, chuyển đổi số, quản trị dữ liệu.

i) Bộ phận văn phòng:

- Tại cơ quan Cục Thuế, Thuế tỉnh, thành phố là Văn phòng.

- Tại Thuế cơ sở là bộ phận được phân công làm công tác hành chính, tổng hợp.

j) Đơn vị cung cấp dịch vụ là tổ chức, doanh nghiệp hoặc cá nhân được cơ

quan thuế ký hợp đồng để thực hiện một số công việc, nhiệm vụ theo yêu cầu của cơ quan thuế.

k) Đơn vị quản lý hợp đồng là đơn vị thuộc cơ quan thuế được phân công thực hiện triển khai hợp đồng với đơn vị cung cấp dịch vụ.

2. Từ ngữ viết tắt:

- CĐS: Công nghệ, chuyển đổi số và tự động hoá.

- DLRR: Quản trị dữ liệu và quản lý rủi ro.

- TCCB: Tổ chức cán bộ.

- QLTT: Quản lý tuân thủ và hỗ trợ người nộp thuế.

- OT (Operational Technology): Là các thiết bị và hệ thống dùng để giám sát, điều khiển và tự động hóa các quy trình vật lý.

- IoT (Internet of Things): Là các thiết bị có khả năng kết nối Internet để thu thập, gửi và nhận dữ liệu.

Điều 3. Mục tiêu, nguyên tắc bảo đảm an toàn thông tin

1. Mục tiêu:

a) Bảo vệ thông tin, hệ thống thông tin của Cục Thuế không bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

b) Bảo đảm hoạt động trên không gian mạng của đơn vị, cá nhân thuộc cơ quan thuế không gây phương hại đến an ninh Quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

2. Nguyên tắc bảo đảm an toàn thông tin:

a) Tuân thủ quy định của pháp luật về an toàn thông tin; bảo vệ bí mật nhà nước, bí mật công tác, dữ liệu cá nhân; giao dịch điện tử và các quy định khác có liên quan. Trường hợp có văn bản quy định cập nhật, thay thế hoặc quy định khác tại văn bản quy phạm pháp luật, quyết định của cấp có thẩm quyền cao hơn thì áp dụng quy định tại văn bản đó.

b) Đảm bảo về an toàn thông tin, đồng thời giảm thiểu ảnh hưởng đến việc triển khai các hoạt động nghiệp vụ.

c) Phân cấp, ủy quyền trách nhiệm bảo đảm an toàn thông tin phù hợp với tổ chức bộ máy và phương thức làm việc của Cục Thuế.

Điều 4. Tiểu ban An toàn thông tin

Tiểu ban An toàn thông tin là bộ phận được thành lập để tham mưu, điều phối và giám sát việc thực hiện công tác bảo đảm an toàn thông tin theo quy định

của Quy chế này.

1. Cục Thuế thành lập Tiểu ban An toàn thông tin:

a) Trưởng Tiểu ban là Cục trưởng Cục Thuế.

b) Phó trưởng Tiểu ban là Phó Cục trưởng Cục Thuế.

c) Thành viên:

- 01 Lãnh đạo của từng đơn vị thuộc Cơ quan Cục Thuế.

- 01 công chức làm thư ký Tiểu ban.

d) Trường hợp cần thiết, Trưởng Tiểu ban quyết định thành lập Tổ giúp việc để hỗ trợ Tiểu ban trong việc nghiên cứu, tham mưu, tổng hợp, đôn đốc, theo dõi và tổ chức triển khai các nhiệm vụ về bảo đảm an toàn thông tin. Thành phần, nhiệm vụ và chế độ làm việc của Tổ giúp việc do Trưởng Tiểu ban quyết định.

2. Thuế tỉnh, thành phố thành lập Tiểu ban An toàn thông tin:

a) Trưởng Tiểu ban là Trưởng Thuế tỉnh, thành phố.

b) Phó trưởng Tiểu ban là Phó trưởng Thuế tỉnh, thành phố.

c) Thành viên:

- 01 Lãnh đạo của từng đơn vị thuộc Thuế tỉnh, thành phố;

- 01 công chức làm thư ký Tiểu ban.

d) Trường hợp cần thiết, Trưởng Tiểu ban quyết định thành lập Tổ giúp việc để hỗ trợ Tiểu ban trong việc nghiên cứu, tham mưu, tổng hợp, đôn đốc, theo dõi và tổ chức triển khai các nhiệm vụ về bảo đảm an toàn thông tin. Thành phần, nhiệm vụ và chế độ làm việc của Tổ giúp việc do Trưởng Tiểu ban quyết định.

3. Chức năng, nhiệm vụ của Tiểu ban:

a) Tiểu ban An toàn thông tin tại Cục Thuế

- Tham mưu giúp Lãnh đạo Cục Thuế về định hướng, chiến lược, chính sách và chương trình bảo đảm an toàn thông tin của Cục Thuế;

- Điều phối công tác bảo đảm an toàn thông tin giữa các đơn vị thuộc Cục Thuế và các đơn vị có liên quan;

- Giám sát việc triển khai Quy chế An toàn thông tin cơ quan thuế; đánh giá tình hình, rủi ro an toàn thông tin và chỉ đạo triển khai các biện pháp khắc phục;

- Chỉ đạo công tác ứng cứu, khắc phục các sự cố an toàn thông tin nghiêm trọng;

- Thực hiện các nhiệm vụ khác do Cục Thuế giao.

b) Tiểu ban An toàn thông tin tại Thuế tỉnh, thành phố

- Tham mưu giúp Lãnh đạo Thuế tỉnh, thành phố về công tác bảo đảm an

toàn thông tin tại đơn vị;

- Điều phối công tác bảo đảm an toàn thông tin giữa các đơn vị thuộc Thuế tỉnh, thành phố;

- Giám sát việc thực hiện Quy chế An toàn thông tin cơ quan thuế tại đơn vị; đánh giá rủi ro an toàn thông tin và tổ chức thực hiện các biện pháp xử lý theo thẩm quyền;

- Chỉ đạo công tác ứng cứu, khắc phục các sự cố an toàn thông tin nghiêm trọng tại Thuế tỉnh, thành phố;

- Báo cáo công tác đảm bảo an toàn thông tin tại Thuế tỉnh, thành phố cho Tiểu ban An toàn thông tin của Cục Thuế;

- Thực hiện các nhiệm vụ khác theo phân công của Cục Thuế và Thuế tỉnh, thành phố.

4. Chế độ làm việc

a) Tiểu ban An toàn thông tin họp định kỳ tối thiểu mỗi quý một lần và họp đột xuất theo yêu cầu của Trưởng Tiểu ban hoặc khi xảy ra sự cố an toàn thông tin nghiêm trọng, phát sinh rủi ro lớn hoặc có yêu cầu của Lãnh đạo cơ quan thuế.

b) Kết luận của Tiểu ban An toàn thông tin là căn cứ để các đơn vị triển khai các nhiệm vụ bảo đảm an toàn thông tin theo chức năng, nhiệm vụ được giao.

c) Các đơn vị thuộc cơ quan thuế có trách nhiệm cung cấp đầy đủ thông tin, hồ sơ và phối hợp với Tiểu ban An toàn thông tin trong quá trình đánh giá rủi ro, kiểm tra, giám sát và xử lý sự cố.

d) Biên bản họp, kết luận của Tiểu ban, báo cáo đánh giá rủi ro, báo cáo xử lý sự cố và các tài liệu liên quan phải được lưu trữ theo quy định của pháp luật và quy định của cơ quan thuế.

Chương II
BẢO ĐẢM AN NINH HỆ THỐNG THÔNG TIN

Điều 5. Quản lý an toàn hạ tầng mạng

1. Kiến trúc hạ tầng mạng

a) Kiến trúc mạng phải được thiết kế phù hợp với quy mô, mức độ quan trọng và yêu cầu bảo vệ của hệ thống thông tin.

b) Kiến trúc mạng phải được xây dựng trên cơ sở áp dụng nguyên tắc phòng thủ nhiều lớp, phân vùng mạng, quyền kết nối tối thiểu, mặc định từ chối và bảo đảm tính sẵn sàng.

c) Kiến trúc mạng phải được tài liệu hóa đầy đủ, bao gồm: Kiến trúc tổng thể, kiến trúc chi tiết. Tài liệu kiến trúc mạng phải được cập nhật khi có thay đổi và được rà soát định kỳ hàng năm.

2. Nguyên tắc xây dựng hạ tầng mạng

a) Hệ thống mạng phải được phân chia thành các vùng mạng phù hợp với quy mô, kiến trúc, chức năng, mục đích sử dụng và mức độ quan trọng của hệ thống nhằm hạn chế truy cập trái phép và giảm thiểu nguy cơ lan truyền sự cố an toàn thông tin. Tại Cục Thuế hệ thống mạng được phân chia tối thiểu các vùng mạng sau: Phân vùng mạng trung gian (DMZ) cung cấp dịch vụ Internet, phân vùng mạng biên kết nối với các đơn vị bên ngoài, phân vùng mạng WAN diện rộng, phân vùng lõi chứa các máy chủ, phân vùng mạng phục vụ việc quản trị hệ thống, phân vùng mạng nội bộ, phân vùng mạng cho môi trường kiểm thử, phân vùng mạng cho người dùng, phân vùng mạng riêng cho kết nối Wifi. Tại Thuế tỉnh, thành phố và Thuế cơ sở hệ thống mạng được phân chia tối thiểu các vùng mạng sau: Phân vùng mạng cho người dùng, phân vùng mạng cho máy chủ, phân vùng mạng cho kết nối Internet (trường hợp có kết nối Internet), phân vùng mạng riêng cho kết nối Wifi.

b) An toàn cơ sở hạ tầng mạng phải đảm bảo tối thiểu:

- Có phương án dự phòng cho các thiết bị mạng chính tại Cục Thuế, Thuế TP Hà Nội và Thuế TP HCM;

- Có phương án phòng chống tấn công từ chối dịch vụ, phòng chống tấn công mạng đối với trung tâm dữ liệu của Cục Thuế;

- Có phương án kiểm soát truy cập giữa các vùng mạng; kiểm soát máy tính người dùng kết nối vào mạng;

- Sử dụng các giao thức truyền nhận, giao thức quản trị được mã hóa theo quy định.

3. Quản lý truy cập từ xa (từ Internet)

a) Trường hợp thực hiện công tác quản trị, hỗ trợ hệ thống từ xa, người dùng phải sử dụng mạng riêng ảo (VPN) do Cục Thuế triển khai. Mạng riêng ảo được cấu hình xác thực đa yếu tố.

b) Trường hợp truy cập các ứng dụng, tài nguyên trong nội bộ từ xa, người dùng phải sử dụng hệ thống truy cập từ xa do Cục Thuế triển khai. Hệ thống truy cập từ xa được cấu hình xác thực đa yếu tố.

c) Máy tính sử dụng truy cập từ xa phải đảm bảo: Được khai báo với hệ thống của cơ quan thuế; hệ điều hành còn được hãng hỗ trợ; được cài đặt chương trình

phần mềm phòng chống mã độc và bật chức năng quét theo thời gian thực, được cập nhật thường xuyên.

4. Quản lý vòng đời thiết bị mạng

a) Trước khi đưa vào vận hành, khai thác, thiết bị phải được thực hiện: Cấu hình an toàn (phân quyền truy cập, thiết lập giới hạn thời gian chờ (timeout); loại bỏ hoặc vô hiệu hóa các tài khoản, dịch vụ, giao thức và cổng kết nối không cần thiết; giới hạn phạm vi truy cập quản trị thiết bị); cứng hóa thiết bị; đánh giá an toàn bảo mật; thực hiện kiểm tra thiết bị; lập danh sách thiết bị.

b) Trong quá trình vận hành:

- Theo dõi, giám sát, kịp thời phát hiện các sự cố về hiệu năng, các sự cố bất thường của các thiết bị;

- Cập nhật các bản vá lỗ hổng, điểm yếu, hệ điều hành;

- Sao lưu cấu hình hiện tại, đánh giá các rủi ro và xây dựng phương án khôi phục khi có sự thay đổi cấu hình hệ thống;

- Rà soát tài khoản và quyền truy cập định kỳ tối thiểu 06 tháng/lần.

c) Kết thúc sử dụng thiết bị: Thiết bị phải được xóa toàn bộ thông tin cấu hình trước khi dừng hoạt động.

Điều 6. Quản lý an toàn máy chủ

1. Máy chủ phải được đặt vào các vùng mạng phù hợp chức năng, mục đích sử dụng và mức độ quan trọng.

2. Quản lý vòng đời máy chủ

a) Trước khi đưa vào vận hành, khai thác, máy chủ phải được: Cấu hình an toàn (phân quyền truy cập, thiết lập giới hạn thời gian chờ (timeout), loại bỏ hoặc vô hiệu hóa các tài khoản, dịch vụ, giao thức và cổng kết nối không cần thiết, giới hạn phạm vi truy cập quản trị máy chủ, cài đặt phần mềm và cấu hình bảo mật theo quy định); cứng hóa thiết bị; đánh giá an toàn bảo mật; lập danh sách máy chủ.

b) Trong quá trình vận hành

- Theo dõi, giám sát, phát hiện các sự cố của máy chủ: hiệu năng CPU, dung lượng lưu trữ, cập nhật nhật ký hệ thống;

- Cập nhật các bản vá lỗ hổng, điểm yếu, phần mềm được cài đặt trên hệ thống máy chủ;

- Sao lưu cấu hình hiện tại, đánh giá các rủi ro và xây dựng phương án khôi phục khi có sự thay đổi cấu hình hệ thống;

- Định kỳ 06 tháng/lần rà soát tài khoản và quyền truy cập.

c) Kết thúc sử dụng máy chủ: Khi thiết bị không còn sử dụng, máy chủ phải được xóa toàn bộ thông tin cấu hình, dữ liệu đảm bảo không có khả năng khôi phục.

Điều 7. Quản lý an toàn ứng dụng

1. Ứng dụng được phát triển hoặc đưa vào sử dụng trong cơ quan thuế phải đáp ứng các yêu cầu sau:

a) Có cơ chế quản lý định danh, xác thực và kiểm soát truy cập phù hợp với chức năng, nhiệm vụ của người sử dụng đáp ứng theo quy định của quy chế này.

b) Bảo vệ thông tin xác thực và dữ liệu nhạy cảm trong quá trình lưu trữ và truyền nhận.

c) Thiết lập cơ chế quản lý phiên làm việc an toàn.

d) Kiểm tra tính hợp lệ của dữ liệu đầu vào và đầu ra trước khi xử lý hoặc cung cấp cho người sử dụng.

đ) Có cơ chế ghi nhật ký các hoạt động của quản trị, các hoạt động quan trọng người sử dụng (tối thiểu gồm: đăng nhập; khai thác, tra cứu thông tin, chỉnh sửa dữ liệu mức L2, L3, L4...).

e) Có biện pháp bảo vệ ứng dụng trước các nguy cơ, lỗ hổng và hình thức tấn công phổ biến.

g) Bảo đảm tính toàn vẹn, xác thực và chống chối bỏ đối với các giao dịch điện tử theo quy định của pháp luật.

2. Môi trường xây dựng ứng dụng

a) Môi trường phát triển, kiểm thử, đào tạo, vận hành chính thức được tách biệt.

b) Không sử dụng dữ liệu thật chứa thông tin nhạy cảm trên môi trường phát triển hoặc kiểm thử, trừ trường hợp dữ liệu đã được biến đổi.

c) Không lưu trữ thông tin xác thực, khóa mật mã, thông tin bí mật hoặc dữ liệu nhạy cảm trực tiếp trong mã nguồn, tập tin cấu hình hoặc kho mã nguồn.

3. Thành phần phần mềm và mã nguồn

a) Việc phát triển phần mềm, bao gồm cả trường hợp sử dụng AI để hỗ trợ, phải bảo đảm an toàn, bảo mật đối với các thành phần, thư viện, nền tảng và dịch vụ được sử dụng. Sử dụng các công cụ hỗ trợ phát triển phần mềm bằng AI phải tuân thủ theo quy định tại Điều 13 Quy chế này.

b) Quản lý danh mục các thành phần phần mềm của bên thứ ba được sử dụng, đánh giá rủi ro và thường xuyên cập nhật các lỗ hổng bảo mật liên quan khi có

thông báo.

c) Sử dụng các thuật toán và cơ chế mật mã đáp ứng quy định của pháp luật.

d) Mã nguồn được quản lý tập trung, kiểm soát phiên bản và bảo vệ khỏi truy cập, sửa đổi hoặc sử dụng trái phép.

4. Đơn vị phát triển phần mềm có trách nhiệm bảo đảm tính bảo mật của thông tin, dữ liệu được tiếp cận trong quá trình thực hiện; không sao chép, sử dụng, tiết lộ hoặc cung cấp cho bên thứ ba khi chưa được cơ quan thuế chấp thuận; chịu trách nhiệm về tính hợp pháp của phần mềm; tuân thủ quy định về quyền sở hữu trí tuệ và các cam kết về bảo mật theo hợp đồng.

5. Vòng đời ứng dụng

a) Trước khi đưa vào vận hành, ứng dụng phải được: Kiểm tra và khắc phục lỗ hổng bảo mật trong mã nguồn, lỗ hổng trong thư viện, thành phần mở rộng (component, extension...); kiểm thử xâm nhập và khắc phục các lỗ hổng bảo mật.

b) Trong quá trình vận hành:

- Theo dõi, giám sát, kịp thời phát hiện các sự cố về hiệu năng, các sự cố bất thường của ứng dụng;

- Cập nhật các bản vá lỗ hổng, điểm yếu, hệ điều hành;

- Sao lưu cấu hình hiện tại, đánh giá các rủi ro và xây dựng phương án khôi phục khi có sự thay đổi cấu hình hệ thống;

- Rà soát tài khoản và quyền truy cập ứng dụng.

c) Kết thúc sử dụng: Khi ứng dụng không còn sử dụng, đơn vị quản lý thông báo cho đơn vị liên quan để thu hồi tài nguyên theo quy định.

Điều 8. Quản lý an toàn dữ liệu

1. Sử dụng phương pháp mã hoá theo quy định của pháp luật để mã hoá các thông tin yêu cầu bảo vệ tại Điều 18 hoặc theo yêu cầu nghiệp vụ.

2. Có phương án an toàn để quản lý và bảo vệ dữ liệu mã hóa, khóa giải mã. Phân quyền truy cập chỉ cho phép người có quyền được truy cập, khai thác dữ liệu mã hóa.

3. Có phương án kiểm tra tính toàn vẹn của thông tin quan trọng, thông tin nhạy cảm trong hệ thống (thông qua hồ sơ giấy, dữ liệu có chữ ký số hoặc mã kiểm tra tính nguyên vẹn).

4. Thực hiện mã hoá đối với các thông tin nhạy cảm trước khi đưa vào phương tiện lưu trữ hoặc trước khi truyền trên đường truyền (khoá giải mã không gửi kèm dữ liệu đã được mã hoá).

5. Đối với các thông tin mật sử dụng các giải pháp truyền nhận do Ban Cơ yếu chính phủ quy định, các đơn vị có văn bản trực tiếp với Ban Cơ yếu chính phủ (Cục Cơ yếu Đảng Chính quyền) để được cấp.

Điều 9. Sao lưu dữ liệu

1. Phạm vi sao lưu dữ liệu tối thiểu bao gồm:

a) Tập tin cấu hình của hệ thống.

b) Bản dự phòng hệ điều hành máy chủ.

c) Cơ sở dữ liệu của các hệ thống thông tin.

d) Dữ liệu và thông tin nghiệp vụ.

đ) Các loại dữ liệu khác theo yêu cầu khi thiết kế hệ thống.

2. Kế hoạch sao lưu dữ liệu được xác định khi xây dựng hệ thống tùy thuộc vào mức độ quan trọng của dữ liệu, trong đó quy định: Tần suất sao lưu, phương pháp sao lưu và thời gian lưu giữ bản sao lưu.

3. Thực hiện sao lưu dữ liệu

a) Thực hiện sao lưu theo lịch trình.

b) Theo dõi và cảnh báo khi xảy ra lỗi trong quá trình sao lưu.

c) Quản lý lịch sử sao lưu và phiên bản dữ liệu sao lưu.

d) Khôi phục dữ liệu khi có yêu cầu.

4. Bảo vệ dữ liệu sao lưu:

a) Không bị sửa đổi, phá hủy hoặc mất mát trái phép.

b) Duy trì khả năng truy cập và khôi phục khi cần thiết.

c) Đảm bảo tính toàn vẹn trong suốt vòng đời lưu trữ.

d) Quyền truy cập, sử dụng và khôi phục dữ liệu sao lưu được phân quyền, kiểm soát và ghi nhận nhật ký.

5. Lưu trữ và quản lý bản sao lưu

a) Các bản sao lưu được định danh, quản lý phiên bản thời gian tạo lập và thời gian lưu giữ.

b) Đối với các hệ thống quan trọng, bản sao lưu phải lưu trữ tách biệt với môi trường vận hành.

6. Kiểm tra khả năng khôi phục dữ liệu: định kỳ hàng năm thực hiện khôi phục dữ liệu một lần.

Điều 10. Quản lý an toàn thiết bị đầu cuối

1. Thiết bị đầu cuối do cơ quan thuế trang bị là máy tính (máy tính để bàn, máy tính xách tay), máy in, thiết bị phát sóng wifi, thiết bị cầm tay thông minh,...

2. Nguyên tắc an toàn với thiết bị đầu cuối:

a) Máy tính phải kết nối với hệ thống tên miền do Cục Thuế triển khai (join domain).

b) Không đăng nhập tài khoản có quyền quản trị trên máy tính (trừ trường hợp phục vụ công tác cài đặt hoặc xử lý lỗi).

c) Không kết nối với hệ thống mạng không dây, mạng dữ liệu di động (3G/4G/5G...) khi đang kết nối hệ thống mạng có dây.

d) Không tự ý cài đặt phần mềm bên ngoài khi chưa được phê duyệt.

đ) Không được kết nối thiết bị lưu trữ di động vào máy tính. Trường hợp người dùng cần sử dụng để phục vụ công việc (xử lý lỗi máy tính, sao lưu dữ liệu lớn,...) phải có sự phê duyệt.

e) Ổ cứng các máy tính xách tay phải được mã hóa.

g) Khoá máy tính ngay khi rời khỏi nơi làm việc; đặt chế độ khoá màn hình máy tính sau 10 phút; tắt máy tính khi rời khỏi cơ quan.

3. Quản lý vòng đời thiết bị đầu cuối

a) Trước khi đưa vào sử dụng thiết bị phải được: Cấu hình an toàn (loại bỏ hoặc vô hiệu hóa các tài khoản, dịch vụ, giao thức và cổng kết nối không cần thiết; giới hạn phạm vi truy cập quản trị thiết bị, cài đặt phần mềm và cấu hình bảo mật theo quy định); thực hiện cứng hóa; đánh giá an toàn bảo mật; lập danh sách thiết bị.

b) Trong quá trình sử dụng:

- Theo dõi, giám sát để kịp thời phát hiện các sự cố, dấu hiệu bất thường ảnh hưởng đến thiết bị đầu cuối trên các hệ thống phần mềm phòng chống mã độc, các hệ thống khác do Cục Thuế triển khai.

- Khi không còn nhu cầu sử dụng, các thiết bị đầu cuối được xoá bỏ cấu hình, dữ liệu trước khi làm thủ tục thu hồi.

- Máy tính phải được xoá toàn bộ dữ liệu bằng phần mềm do Cục Thuế triển khai khi: Chuyển sử dụng từ cá nhân này sang cá nhân khác; không tiếp tục sử dụng cho công việc của cơ quan. Trường hợp máy tính đưa ra ngoài cơ quan để bảo hành, bảo dưỡng, sửa chữa, ổ cứng phải được tháo rời trước khi bàn giao cho đơn vị cung cấp dịch vụ. Đối với ổ cứng gửi bảo hành, sửa chữa hoặc thay thế, cần thực hiện xóa toàn bộ dữ liệu trước khi bàn giao; trường hợp không thể xóa dữ liệu, cần áp dụng biện pháp bảo vệ phù hợp để ngăn chặn việc truy cập dữ liệu.

- Cập nhật vào thông tin quản lý tài sản khi thiết bị kết thúc sử dụng.

4. Quản lý và sử dụng máy tính soạn thảo văn bản chứa nội dung bí mật nhà nước:

a) Sử dụng hệ điều hành và các phần mềm soạn thảo văn bản có bản quyền; không kết nối vào mạng (Internet, nội bộ, không dây), trừ trường hợp đã áp dụng các biện pháp bảo vệ theo hướng dẫn của Ban Cơ yếu Chính phủ; chỉ sử dụng thiết bị lưu trữ mật do Ban Cơ yếu Chính phủ cung cấp.

b) Phân quyền truy cập máy tính theo tên người truy cập được giao soạn thảo bí mật nhà nước.

c) Trường hợp ổ cứng lỗi cần bảo hành, phải thực hiện biện pháp xóa toàn bộ dữ liệu trước khi mang ổ cứng ra khỏi cơ quan và có biên bản ghi nhận về việc xóa dữ liệu giữa đơn vị sử dụng máy tính và đơn vị nhận ổ cứng. Việc sửa chữa, nâng cấp phần mềm cho máy tính (sau khi đã đưa vào sử dụng) được thực hiện dưới sự giám sát của đơn vị sử dụng máy tính, bảo đảm không để lộ, lọt dữ liệu trên ổ cứng máy tính ra bên ngoài.

5. Quy định về thiết bị đầu cuối do người dùng tự trang bị:

- Không được kết nối vào hệ thống mạng nội bộ có dây của cơ quan thuế.

- Máy tính sử dụng truy cập từ xa phải bảo đảm: Được khai báo với hệ thống của cơ quan thuế; hệ điều hành còn được hãng hỗ trợ; được cài đặt chương trình phần mềm phòng chống mã độc và bật chức năng quét theo thời gian thực và được cập nhật thường xuyên.

Điều 11. Quản lý an toàn người sử dụng

1. Chỉ lưu trữ thông tin, dữ liệu phục vụ công việc trên ổ đĩa mạng; phải xóa các thông tin, dữ liệu do mình tạo ra khi hết thời hạn lưu trữ hoặc không còn giá trị sử dụng theo quy định; không để lộ thông tin công việc, dữ liệu người nộp thuế hoặc thông tin nhạy cảm trên màn hình máy tính; không để tài liệu chứa thông tin mật, thông tin người nộp thuế hoặc dữ liệu nhạy cảm tại bàn sau giờ làm việc (tài liệu phải được cất giữ trong tủ hoặc khu vực lưu trữ phù hợp).

2. Không tự ý sử dụng các công cụ để cập nhật dữ liệu tự động theo lô lớn làm tắc nghẽn hệ thống. Trường hợp sử dụng công cụ để phục vụ việc khai thác, cập nhật dữ liệu cho công việc thì phải được phê duyệt của Cục Thuế.

3. Đối với các dữ liệu quan trọng, nhạy cảm cần phải đặt mật khẩu khi lưu trữ hoặc khi gửi ra bên ngoài. Gửi mật khẩu cho người nhận không kèm với tệp tin. Mật khẩu bao gồm ký tự viết thường, ký tự viết hoa, ký tự đặc biệt, chữ số, độ dài tối thiểu 14 ký tự.

4. Chỉ sử dụng thư điện tử công vụ để phục vụ công việc. Không được phép cho người khác sử dụng tài khoản của mình và không được phép sử dụng tài khoản của người khác dưới bất kỳ hình thức nào. Không được phép lắp đặt các thiết bị cá

nhân (điện thoại, thiết bị mạng, thiết bị viễn thông (4G/5G)) vào hệ thống mạng nội bộ của cơ quan khi chưa được sự phê duyệt.

5. Trường hợp phát hiện máy tính bị nhiễm mã độc thì người dùng cần thông báo ngay cho bộ phận CNTT để xử lý.

6. Trường hợp phát hiện có dấu hiệu tài khoản bị lộ lọt, thông tin quan trọng, nhạy cảm bị tiết lộ, người dùng cần thay đổi mật khẩu và thông báo ngay cho bộ phận CNTT để có biện pháp xử lý.

7. Phối hợp với bộ phận CNTT thực hiện các biện pháp an toàn thông tin mạng trên máy tính của người dùng.

8. Đối với các dữ liệu được dán nhãn L2, L3 theo quy định tại khoản 3 Điều 18 Quy chế này, người dùng phải thực hiện lưu trữ dữ liệu tập trung trên hệ thống sao lưu của cơ quan thuế.

Điều 12. Quản lý an toàn tài khoản và quyền truy cập

1. Tài khoản là tập hợp gồm tên đăng nhập và mật khẩu hoặc hình thức xác thực khác, được gắn với quyền truy cập thực hiện một số tác vụ trên hệ thống thông tin hoặc trên thiết bị xử lý thông tin, bao gồm các loại sau:

a) Tài khoản định danh (tài khoản của người dùng cuối) được cấp cho một người dùng duy nhất và được gắn quyền truy cập các hệ thống thông tin.

b) Tài khoản chức năng dùng để truy cập hệ thống gắn với một nhiệm vụ cụ thể để thực hiện nhiệm vụ của cơ quan (ví dụ: Tài khoản văn thư, tài khoản biên tập,...). Tài khoản này phải được bàn giao cho công chức, viên chức, người lao động cụ thể quản lý. Khi kết thúc thời gian thực hiện nhiệm vụ, người dùng bàn giao tài khoản chức năng cho người dùng được phân công tiếp nhận nhiệm vụ hoặc bàn giao tài khoản cho đơn vị quản lý người dùng.

c) Tài khoản kỹ thuật là tài khoản chỉ được thực hiện xác thực giữa các ứng dụng hoặc ứng dụng với cơ sở dữ liệu. Không cho phép người dùng tương tác/đăng nhập trực tiếp.

d) Tài khoản quản trị là tài khoản có quyền cài đặt, cấu hình các thông số và cấp quyền truy cập trên hệ thống thông tin. Tài khoản quản trị được giao cho cá nhân, đơn vị thực hiện nhiệm vụ quản trị ứng dụng, quản trị cơ sở dữ liệu, quản trị hệ điều hành, quản trị thiết bị. Trường hợp thuê ngoài, đơn vị chủ trì quản lý: lập danh sách cá nhân được giao tài khoản quản trị; thời điểm cá nhân tiếp nhận/kết thúc sử dụng; cập nhật danh sách khi có thay đổi về nhân sự giữ tài khoản.

2. Quy định về quản lý tài khoản:

a) Mỗi tài khoản truy cập phải được gán cho một người quản lý/sử dụng duy nhất. Cá nhân được cấp hoặc giao quản lý tài khoản chịu trách nhiệm về các hành vi của tài khoản được ghi nhận trên thiết bị xử lý thông tin, hệ thống thông tin, hệ thống giám sát an toàn thông tin mạng. Trường hợp chia sẻ tài khoản dùng chung, phải mô tả rõ trách nhiệm của mỗi cá nhân tại thời điểm sử dụng và được phê duyệt bởi lãnh đạo cơ quan thuế.

b) Mỗi tài khoản chỉ được cấp quyền tối thiểu. Việc cấp tài khoản và quyền truy cập tuân thủ quy định của nghiệp vụ, quy trình cấp mới, thay đổi và thu hồi quyền truy cập vào các tài sản của cơ quan, tổ chức.

c) Thay đổi hoặc vô hiệu hóa tài khoản mặc định trên phần mềm, thiết bị (tài khoản root, administrator, tài khoản cấu hình sẵn của nhà cung cấp dịch vụ).

d) Các loại tài khoản sau phải được tách biệt không sử dụng chung một tài khoản: Tài khoản quản trị, tài khoản hệ thống, tài khoản người dùng, tài khoản kỹ thuật, tài khoản dịch vụ.

đ) Tài khoản (trừ tài khoản hệ thống, tài khoản kỹ thuật) bị tạm khoá trong thời gian 05 phút nếu đăng nhập sai quá 05 lần liên tục.

e) Xoá hoặc vô hiệu hoá các tài khoản không hoạt động sau 45 ngày hoặc ngay khi có thay đổi nhân sự quản lý tài khoản hoặc nhân sự quản lý tài khoản bị nghi ngờ có hành vi vi phạm an toàn thông tin.

3. Quy định về mật khẩu:

a) Mật khẩu gồm: Ký tự viết thường, ký tự viết hoa, ký tự đặc biệt, chữ số, không chứa tên tài khoản và có tối thiểu 14 ký tự.

b) Mật khẩu phải được giữ bí mật, thay đổi trong lần đăng nhập đầu tiên (trừ tài khoản hệ thống, tài khoản kỹ thuật) và định kỳ 06 tháng/01 lần. Riêng tài khoản quản trị thay đổi mật khẩu định kỳ 02 tháng/01 lần. Mật khẩu mới không được trùng với 10 mật khẩu trước đó.

c) Mật khẩu của tài khoản thay thế tài khoản root/administrator phải được đóng phong bì kín bàn giao cho Lãnh đạo bộ phận CNTT và được lưu trong tủ cá nhân có khóa.

4. Quy định về xác thực đa nhân tố:

a) Các hệ thống cho phép truy cập từ Internet đối với người dùng công chức cơ quan thuế, người dùng là quản trị, hỗ trợ bắt buộc sử dụng tối thiểu xác thực 2 yếu tố.

b) Ưu tiên sử dụng xác thực tối thiểu 2 yếu tố để tăng cường an toàn bảo mật đối với các hệ thống quan trọng.

5. Thiết lập và duy trì hệ thống quản lý tài khoản:

a) Lập danh sách tài khoản thiết bị/phần mềm.

b) Danh sách tài khoản bao gồm các thông tin: loại tài khoản, tên tài khoản, trạng thái tài khoản, tên thiết bị/phần mềm, địa chỉ IP, tên người quản lý, phòng ban, ngày kích hoạt tài khoản, ngày vô hiệu hoá tài khoản (nếu có).

c) Danh sách tài khoản phải được rà soát định kỳ tối thiểu 01 lần/quý, loại bỏ các tài khoản không sử dụng, các tài khoản không còn hợp lệ trên hệ thống thông tin.

Điều 13. Quản lý an toàn sử dụng các công cụ trí tuệ nhân tạo (Artificial Intelligence - AI)

1. Việc sử dụng các công cụ trí tuệ nhân tạo (AI) trong quá trình xử lý công việc phải bảo đảm tuân thủ các quy định về bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân, bảo vệ thông tin của người nộp thuế.

2. Nghiêm cấm nhập, tải lên hoặc chia sẻ với các công cụ AI công cộng hoặc các dịch vụ AI của bên thứ ba các thông tin sau (trừ trường hợp được cấp có thẩm quyền phê duyệt hoặc hệ thống AI được triển khai trong môi trường do cơ quan thuế quản lý và đáp ứng đầy đủ các yêu cầu về an toàn thông tin):

a) Bí mật nhà nước.

b) Thông tin của người nộp thuế.

c) Dữ liệu trao đổi theo điều ước hoặc thỏa thuận quốc tế.

d) Dữ liệu cá nhân.

đ) Mã nguồn, khóa mật mã, mật khẩu, chứng thư số, khóa API, thông tin xác thực hoặc các thông tin có thể ảnh hưởng đến an toàn hệ thống.

Điều 14. Phòng ngừa, phát hiện và ứng phó với mã độc

1. Máy tính, máy chủ (trừ máy tính mật, các máy chủ cài đặt hệ điều hành) và các thiết bị di động (nếu có) phải được cài đặt phần mềm phòng chống mã độc do Cục Thuế cung cấp. Giải pháp phòng, chống mã độc, bao gồm các tính năng cơ bản: Bảo vệ thời gian thực, tự động cập nhật các mẫu nhận diện mã độc mới, tính năng phòng chống khai thác lỗ hổng (IPS). Riêng các máy tính ngoài trụ sở cơ quan thuế, trường hợp không cập nhật được tự động thì định kỳ hàng tuần máy tính phải được cập nhật thủ công các bản nâng cấp mới nhất. Thông tin cảnh báo thiết bị nhiễm mã độc phải được chuyển về hệ thống giám sát an toàn thông tin 24/7.

2. Không được tự ý vô hiệu hóa, gỡ bỏ hoặc thay đổi cấu hình các giải pháp phòng chống mã độc do Cục Thuế triển khai.

3. Các phần mềm trước khi cài đặt trên máy tính, các file trao đổi qua môi trường mạng đều phải được kiểm tra bằng phần mềm phòng chống mã độc. Thực hiện rà quét mã độc và vô hiệu hoá tính năng tự động thực thi đối với các phương tiện lưu trữ.

4. Định kỳ thực hiện dò quét tìm kiếm phần mềm mã độc còn tồn tại trên toàn bộ thiết bị (máy tính 01 tuần/lần, máy chủ 01 tháng/lần).

5. Khi phát hiện thiết bị có dấu hiệu nhiễm mã độc hoặc bị khai thác trái phép, người sử dụng cô lập thiết bị khỏi mạng, dừng dịch vụ hoặc ngắt kết nối để ngăn chặn nguy cơ lây lan và thông báo ngay cho bộ phận CNTT.

6. Hàng ngày (ngày làm việc) truy cập hệ thống quản lý phần mềm phòng chống mã độc để kiểm tra hoạt động hệ thống, kịp thời phát hiện và xử lý các máy tính có dấu hiệu nhiễm mã độc.

7. Triển khai các giải pháp phát hiện, điều tra và ứng phó mối đe dọa trên thiết bị đầu cuối (EDR/XDR) nhằm nâng cao khả năng phát hiện và xử lý mã độc nâng cao.

Điều 15. Quản lý lỗ hổng bảo mật

1. Khi phát hiện lỗ hổng bảo mật (thông qua phần mềm quản lý lỗ hổng, thông qua rà quét lỗ hổng định kỳ, thông qua thông báo từ các cơ quan chức năng như Bộ Công an, Bộ Quốc phòng, Bộ Tài chính…), Ban CĐS thực hiện phân loại điểm yếu và thông báo đến các đơn vị, bộ phận thông qua thư điện tử.

2. Khi có thông tin về lỗ hổng bảo mật, đơn vị vận hành/đơn vị quản lý thiết bị/tài sản thực hiện:

a) Phối hợp các đơn vị liên quan để phân tích đánh giá tác động, ưu tiên các điểm yếu "Nghiêm trọng" có mã khai thác, lên kế hoạch, tổ chức kiểm thử, xây dựng phương án phục hồi trước khi tiến hành triển khai và xử lý các điểm yếu. Các điểm yếu an toàn thông tin chưa thể xử lý ngay, đơn vị vận hành phối hợp Ban CĐS có phương án xử lý tạm thời cho các điểm yếu an toàn thông tin.

b) Thực hiện cập nhật bản vá cho hệ thống, thiết bị và thông báo kết quả cho Ban CĐS.

Điều 16. Quản lý an toàn kết nối Internet và thư điện tử

1. Quản lý an toàn truy cập Internet

a) Người sử dụng khi truy cập Internet từ mạng nội bộ có dây cơ quan thuế phải sử dụng trình duyệt web qua hệ thống truy cập Internet do Cục Thuế triển khai. Việc kết nối, truy cập và sử dụng Internet chỉ phục vụ hoạt động công vụ, quản lý, vận hành, đào tạo và các nhiệm vụ được giao.

Người sử dụng không được: Tự ý thiết lập các kết nối Internet; sử dụng các phần mềm, dịch vụ hoặc công cụ nhằm che giấu, thay đổi hoặc chuyển hướng lưu lượng truy cập Internet trái quy định.

b) Máy chủ, thiết bị mạng, thiết bị bảo mật khi kết nối Internet để cập nhật bản vá, chữ ký nhận diện, cơ sở dữ liệu bảo mật hoặc các thông tin từ nhà sản xuất phải thực hiện thông qua hệ thống truy cập Internet do Cục Thuế triển khai. Đối với các thiết bị không thể thực hiện thông qua hệ thống truy cập qua Internet tập trung, các thiết bị sẽ được mở kết nối trực tiếp nhưng hạn chế đến địa chỉ và cổng cụ thể.

c) Hệ thống kết nối Internet phải đảm bảo có tính năng rà quét phòng chống mã độc, có các bộ lọc URL để ngăn chặn kết nối với các trang web độc hại tiềm ẩn hoặc không được chấp thuận.

d) Cục Thuế công bố danh sách các trình duyệt web an toàn, danh sách địa chỉ trang thông tin điện tử được phép truy cập. Trường hợp đơn vị có yêu cầu truy cập trang thông tin điện tử không nằm trong danh sách đã công bố, Thuế tỉnh/thành phố gửi văn bản đề nghị về Cục Thuế (qua Ban CĐS).

2. Quản lý an toàn dịch vụ thư điện tử

a) Triển khai giải pháp ngăn chặn việc gửi, nhận các tệp đính kèm có khả năng thực thi mã hoặc gây mất an toàn thông tin.

b) Triển khai giải pháp bảo vệ phòng chống mã độc, bảo vệ phòng chống thư giả mạo (phishing email), thư rác (spam mail), phát hiện, cảnh báo và ngăn chặn các thư điện tử chứa liên kết độc hại, liên kết lừa đảo (phishing), liên kết giả mạo.

c) Định kỳ hàng tháng rà quét và cập nhật điểm yếu cho dịch vụ thư điện tử.

Điều 17. Giám sát an ninh hệ thống thông tin

1. Hệ thống giám sát an toàn thông tin 24/7 đảm bảo: Thu thập nhật ký từ các thiết bị; được theo dõi, vận hành hàng ngày. Nhật ký được: Rà soát đánh giá điểm yếu tối thiểu 03 tháng/lần; rà soát nhật ký tối thiểu 01 lần/tuần và lưu trữ tối thiểu 12 tháng.

2. Tất cả máy chủ, ứng dụng, thiết bị mạng, thiết bị an toàn thông tin, hệ điều hành, cơ sở dữ liệu phải được cấu hình chức năng ghi nhật ký (logging) trong suốt quá trình vận hành. Không được tắt, vô hiệu hóa hoặc làm gián đoạn chức năng ghi nhật ký, trừ trường hợp bảo trì, nâng cấp hoặc xử lý sự cố theo quy trình được phê duyệt.

3. Các loại nhật ký được thu thập gồm: Nhật ký truy cập hệ thống, nhật ký tiến trình hoạt động, nhật ký ứng dụng, nhật ký cảnh báo của các thiết bị bảo mật.

Thông tin nhật ký gồm:

- Địa chỉ nguồn (IP/ tên máy/tên miền), địa chỉ đích (IP/ tên máy/tên miền), tài khoản đích (tên người dùng/ mã định danh), thời điểm truy cập đối với truy cập hệ thống.

- Thông tin thiết bị (IP/ tên thiết bị/tên miền), thông tin tiến trình, tài khoản đích (tên người dùng/ mã định danh), thời điểm xảy ra đối với tiến trình hoạt động.

- Tài khoản người dùng (tên người dùng/mã định danh), địa chỉ nguồn (IP/tên máy), chức năng hoặc giao dịch được thực hiện, đối tượng dữ liệu bị tác động (nếu có), kết quả thực hiện (thành công/thất bại) (nếu có), thời điểm xảy ra đối với ứng dụng.

- Tên cảnh báo, thiết bị, mức độ, địa chỉ nguồn, loại cảnh báo, thời điểm xảy ra đối với cảnh báo của các thiết bị bảo mật.

4. Các hệ thống thông tin từ cấp độ 3 trở lên, hệ thống giám sát, thiết bị hạ tầng truyền thông, thiết bị bảo mật tại Cục Thuế phải được cấu hình gửi nhật ký về hệ thống giám sát trước khi đưa vào hoạt động. Thời gian của hệ thống giám sát và đối tượng giám sát phải được đồng bộ với máy chủ thời gian của Cục Thuế.

5. Hệ thống giám sát thiết lập các cảnh báo để phát hiện các dấu hiệu tấn công, các vi phạm, các dấu hiệu bất thường, các rủi ro của hệ thống. Đơn vị giám sát thực hiện phân tích, xác minh và chuyển cảnh báo đến đơn vị hoặc cá nhân quản lý, vận hành hệ thống để kịp thời kiểm tra, xử lý và khắc phục.

6. Khi phát hiện hoặc nghi ngờ xảy ra sự cố an toàn thông tin, đơn vị vận hành hệ thống giám sát 24/7 thực hiện bảo vệ, lưu giữ nguyên trạng nhật ký để khắc phục sự cố. Chỉ cá nhân được phân công mới được truy cập, khai thác các nhật ký này.

Chương III
PHÂN LOẠI VÀ BẢO ĐẢM AN NINH DỮ LIỆU

Điều 18. Phân loại dữ liệu và bảo vệ theo mức độ

1. Nguyên tắc phân loại dữ liệu

a) Dữ liệu được phân loại căn cứ mức độ thiệt hại có thể xảy ra đối với Nhà nước, cơ quan thuế, tổ chức, cá nhân nếu dữ liệu bị lộ lọt, sửa đổi hoặc mất mát trái phép, không phụ thuộc định dạng (giấy, điện tử) hay nơi lưu trữ.

b) Người tạo lập, thu thập hoặc trực tiếp quản lý dữ liệu có trách nhiệm đề xuất mức phân loại ban đầu; thủ trưởng đơn vị trực tiếp quản lý dữ liệu phê duyệt mức phân loại, trừ trường hợp dữ liệu đã được cấp có thẩm quyền cao hơn ấn định

mức bảo vệ theo quy định pháp luật khác (bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân...).

c) Việc thu thập, phân loại dữ liệu phải tuân thủ nguyên tắc đúng mục đích, giới hạn ở phạm vi cần thiết để thực hiện chức năng, nhiệm vụ được giao.

2. Phân loại dữ liệu

Dữ liệu được phân loại thành các loại như sau: Sử dụng rộng rãi, sử dụng nội bộ, sử dụng hạn chế và sử dụng đặc biệt hạn chế.

3. Quy định bảo mật với từng loại dữ liệu:

a) Dữ liệu được phân loại sử dụng rộng rãi:

- Dữ liệu được dán nhãn: L0.

- Quy định truy cập: Người bên trong và bên ngoài cơ quan thuế có thể sử dụng.

- Lưu trữ dữ liệu:

+ Dữ liệu dạng giấy: Không quy định.

+ Dữ liệu điện tử: Không quy định.

- Sao chép và in ấn: Không quy định.

- Trao đổi qua kênh điện tử: Không quy định.

- Tiêu hủy dữ liệu: Không quy định.

b) Dữ liệu được phân loại sử dụng nội bộ:

- Dữ liệu được dán nhãn: L1.

- Quy định truy cập: Chỉ công chức thuế mới được phép tiếp cận.

- Lưu trữ dữ liệu:

+ Dữ liệu dạng giấy: Để trong khu vực nội bộ cơ quan thuế.

+ Dữ liệu điện tử: Lưu trữ trên mạng nội bộ hoặc lưu trữ trong các thiết bị lưu trữ di động của công chức được giao nhiệm vụ hoặc lưu trữ trong các thiết bị lưu trữ di động của cơ quan thuế.

- Sao chép và in ấn: Được sao chép và in ấn để phân phát trong nội bộ; tài liệu giấy được gắn nhãn sử dụng nội bộ; không mang ra ngoài trụ sở cơ quan thuế nếu mang ra ngoài phải được người có thẩm quyền cho phép và thực hiện biện pháp bảo vệ phù hợp.

- Trao đổi qua kênh điện tử: Có thể gửi qua các kênh điện tử nội bộ; đường truyền trao đổi thông tin phải có mã hóa.

- Tiêu hủy dữ liệu: Xé vụn bằng tay hoặc sử dụng máy; đối với dữ liệu điện tử cần được xoá trên các thiết bị lưu trữ.

c) Dữ liệu được phân loại sử dụng hạn chế:

- Dữ liệu được dán nhãn: L2.

- Quy định truy cập: Chỉ công chức được giao nhiệm vụ hoặc đơn vị được phân công mới được tiếp cận dữ liệu.

- Lưu trữ dữ liệu:

+ Dữ liệu dạng giấy: Để trong ngăn kéo hoặc tủ có khóa của cơ quan hoặc trong phòng làm việc nhưng việc ra vào phòng có sự kiểm soát.

+ Dữ liệu điện tử: Lưu trữ trong mạng nội bộ và phải được lưu riêng biệt so với dữ liệu khác. Chỉ lưu trữ trong các thiết bị lưu trữ di động của công chức được phép truy cập dữ liệu. Thiết bị lưu trữ di động được mã hóa hoặc việc truy cập thiết bị lưu trữ đặt mật khẩu.

- Sao chép và in ấn: Chỉ được sao chép và in ấn bởi công chức được giao nhiệm vụ hoặc đơn vị được phân công; tài liệu giấy được gắn nhãn sử dụng hạn chế; tài liệu in ấn, copy không để trên bàn làm việc hoặc để tại máy in.

- Trao đổi qua kênh điện tử: Dữ liệu điện tử được gửi qua các kênh email nội bộ để sử dụng giữa các công chức hoặc đơn vị được phân công. Dữ liệu gửi ra ngoài phải được mã hóa hoặc đặt mật khẩu (thông tin khóa giải mã, mật khẩu không được gửi kèm dữ liệu); Đường truyền trao đổi thông tin phải có mã hóa.

- Tiêu hủy dữ liệu: Đối với dữ liệu giấy sử dụng máy xén; đối với dữ liệu điện tử, xoá vĩnh viễn; việc tiêu hủy phải có biên bản.

d) Dữ liệu được phân loại sử dụng đặc biệt hạn chế:

- Dữ liệu được dán nhãn: L3.

- Quy định truy cập: Chỉ công chức được phân công mới được tiếp cận dữ liệu.

- Lưu trữ dữ liệu:

+ Dữ liệu dạng giấy: Để trong ngăn kéo hoặc tủ có khóa đặt tại phòng làm việc có khóa ra vào, có camera giám sát.

+ Dữ liệu điện tử: Dữ liệu được mã hóa trong mạng nội bộ và được lưu riêng biệt so với dữ liệu khác; không được phép lưu trữ trong các thiết bị lưu trữ di động của công chức. Dữ liệu chỉ được lưu trong thiết bị lưu trữ di động đã được mã hóa.

- Sao chép và in ấn: Dữ liệu chỉ được sao chép và in ấn khi được phép; việc sao chép và in ấn phải được ghi chép vào sổ gồm: số bản sao chép và in ấn; người sao chép và mục đích thực hiện; các tài liệu sao chép và in ấn phải được đánh nhãn "dữ liệu cực kỳ hạn chế"; việc sao chép và in ấn phải thực hiện bởi công chức được phân công.

- Trao đổi qua kênh điện tử: Dữ liệu được gửi qua email cơ quan thuế giữa các công chức được tiếp cận. Dữ liệu gửi ra ngoài phải được mã hóa hoặc đặt mật

khẩu (thông tin khóa giải mã, mật khẩu không được gửi kèm dữ liệu). Đường truyền trao đổi thông tin phải có mã hóa.

- Tiêu hủy dữ liệu: Đối với dữ liệu giấy sử dụng máy xén giấy vụn đa chiều; đối với dữ liệu điện tử sử dụng các công cụ để xoá vĩnh viễn hoặc tiêu huỷ phương tiện lưu trữ, đảm bảo không thể khôi phục dữ liệu. Việc tiêu hủy phải có biên bản và có mặt của công chức được phân công tiếp cận dữ liệu.

4. Vòng đời dữ liệu

a) Thu thập: Dữ liệu chỉ được thu thập khi có cơ sở pháp lý hoặc phục vụ trực tiếp chức năng, nhiệm vụ được giao; không thu thập vượt quá phạm vi cần thiết.

b) Thời hạn lưu giữ: Từng loại dữ liệu phải được xác định thời hạn lưu giữ theo quy định của pháp luật về lưu trữ, quy định nghiệp vụ chuyên ngành thuế. Hết thời hạn lưu giữ mà dữ liệu không còn giá trị sử dụng và không thuộc diện lưu trữ vĩnh viễn theo quy định của pháp luật về lưu trữ, đơn vị quản lý dữ liệu tổ chức tiêu hủy theo quy định tại khoản 3 Điều này hoặc chuyển giao cho cơ quan lưu trữ có thẩm quyền.

c) Tái phân loại, giải mật: Định kỳ hằng năm hoặc khi có sự kiện làm thay đổi tính chất của dữ liệu (ví dụ: Thông tin đã được công khai theo quyết định của cấp có thẩm quyền, kết luận thanh tra/kiểm tra đã công bố), đơn vị quản lý dữ liệu rà soát, đề xuất cấp có thẩm quyền quyết định nâng hoặc hạ mức phân loại.

5. Dữ liệu cá nhân

a) Việc thu thập, xử lý dữ liệu cá nhân của người nộp thuế và cá nhân khác trong quá trình thực hiện nhiệm vụ phải tuân thủ quy định của pháp luật về bảo vệ dữ liệu cá nhân. Dữ liệu cá nhân nhạy cảm áp dụng mức bảo vệ tối thiểu L2; trường hợp pháp luật có yêu cầu bảo vệ cao hơn thì áp dụng mức L3.

b) Đối với hoạt động xử lý dữ liệu cá nhân quy mô lớn (xây dựng kho dữ liệu tập trung, mô hình chấm điểm rủi ro tuân thủ trên diện rộng...), đơn vị chủ trì lập hồ sơ đánh giá tác động xử lý dữ liệu cá nhân theo quy định của pháp luật về bảo vệ dữ liệu cá nhân trước khi triển khai; trình cấp có thẩm quyền phê duyệt và lưu giữ phục vụ công tác kiểm tra.

6. Dữ liệu phục vụ phân tích, tổng hợp quy mô lớn

a) Đối với dữ liệu được trích xuất, tổng hợp phục vụ phân tích rủi ro, thống kê, huấn luyện mô hình phân tích dữ liệu thì áp dụng biện pháp mã hóa hoặc giả danh hóa (che, mã hóa một chiều các trường định danh trực tiếp) khi mục đích phân tích không yêu cầu xác định danh tính cụ thể.

b) Trường hợp bắt buộc phải giữ nguyên trường định danh để phục vụ nghiệp

vụ (ví dụ: Lập danh sách người nộp thuế rủi ro cao để thanh tra, kiểm tra), dữ liệu áp dụng mức bảo vệ tương ứng với dữ liệu, không được hạ mức bảo vệ vì lý do phục vụ phân tích.

c) Quyền truy cập vào các kho dữ liệu tổng hợp, hệ thống phân tích dữ liệu lớn phải được ghi nhận nhật ký truy vấn, phục vụ truy vết khi cần thiết.

7. Biện pháp kỹ thuật hỗ trợ gắn nhãn và kiểm soát dữ liệu

a) Triển khai giải pháp gắn nhãn dữ liệu tự động và giải pháp ngăn ngừa thất thoát dữ liệu (Data Loss Prevention) đối với dữ liệu phân loại từ mức L2 trở lên, đặc biệt tại các kênh có nguy cơ rò rỉ cao (thư điện tử, thiết bị lưu trữ di động, tải lên Internet).

b) Cảnh báo từ giải pháp ngăn ngừa thất thoát dữ liệu được đơn vị chuyên trách an toàn hệ thống thông tin xử lý theo quy định.

8. Chất lượng dữ liệu: Đơn vị quản lý dữ liệu có trách nhiệm áp dụng biện pháp phù hợp để dữ liệu được thu thập, cập nhật chính xác, đầy đủ, kịp thời, giảm thiểu sai sót trong quá trình nhập liệu, xử lý; định kỳ rà soát, đối chiếu đối với dữ liệu quan trọng phục vụ công tác quản lý thuế.

9. Xử lý sự cố đối với dữ liệu phân loại mức cao: Sự cố an toàn thông tin liên quan đến dữ liệu phân loại mức L2, L3 phải được ưu tiên xử lý ở mức cao nhất; đơn vị chuyên trách an toàn thông tin xác định phạm vi, mức độ ảnh hưởng và báo cáo Lãnh đạo đơn vị trong thời hạn quy định.

10. Trường hợp quy định truy cập khác với quy định nêu trên phải được sự phê duyệt của các cấp có thẩm quyền.

Chương IV
BẢO ĐẢM AN NINH THÔNG TIN CON NGƯỜI

Điều 19. Bảo đảm an ninh thông tin đối với người dùng là công chức, viên chức, người lao động đang làm việc tại cơ quan thuế

1. Khi tuyển dụng, tiếp nhận hoặc bố trí công tác đối với công chức

a) Việc tuyển dụng, tiếp nhận, điều động, biệt phái hoặc bố trí làm việc đối với các vị trí có quyền truy cập vào hệ thống thông tin, dữ liệu hoặc tài sản thông tin của cơ quan thuế phải được thực hiện theo quy định. Công chức được tuyển dụng vào vị trí công việc về an toàn thông tin phải có bằng tốt nghiệp từ đại học trở lên với các ngành đào tạo về công nghệ thông tin. Đối với công chức được phân công thực hiện công việc liên quan đến trao đổi thông tin theo Điều ước quốc tế về Thuế, cần phải có lý lịch tư pháp.

b) Ban TCCB/Phòng TCCB chủ trì tổ chức ký cam kết bảo vệ bí mật thông tin với công chức trước khi giao nhiệm vụ; đồng thời, phối hợp với các đơn vị liên quan tổ chức đào tạo về an toàn bảo mật cho công chức.

c) Công chức thực hiện ký cam kết bảo vệ bí mật thông tin theo quy định và nghĩa vụ bảo vệ bí mật Nhà nước, bí mật công tác, dữ liệu và các thông tin thuộc phạm vi quản lý của cơ quan thuế vẫn được duy trì sau khi chuyển công tác, nghỉ hưu, thôi việc theo quy định của pháp luật và các cam kết đã ký.

d) Việc cấp quyền truy cập chỉ được thực hiện sau khi hoàn thành các yêu cầu quy định tại điểm b khoản này và được cấp có thẩm quyền phê duyệt.

2. Trong quá trình làm việc

a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ phải đăng ký và được phân quyền chặt chẽ; không đăng nhập máy tính bằng tài khoản quản trị trừ trường hợp đăng nhập để thực hiện công việc chuyên môn; máy tính truy cập, sử dụng tài nguyên nội bộ phải đáp ứng quy định tại Quy chế này.

b) Đơn vị quản lý trực tiếp có trách nhiệm phối hợp với bộ phận CNTT trong việc đề nghị cấp mới, thay đổi, tạm dừng hoặc thu hồi quyền truy cập ứng dụng khi có thay đổi về chức năng, nhiệm vụ hoặc vị trí công tác theo quy định phân quyền. Bộ phận văn phòng đề nghị cấp mới, thay đổi, tạm dừng, thu hồi hoặc khôi phục quyền truy cập vật lý theo quy định khi có thay đổi về người lao động.

c) Khi phát hiện hoặc tiếp nhận thông tin về việc người sử dụng có dấu hiệu vi phạm quy định về an toàn thông tin, vi phạm quy định về bảo vệ dữ liệu, có hành vi sử dụng trái phép hệ thống thông tin hoặc có nguy cơ gây mất an toàn thông tin, đơn vị quản lý trực tiếp thông báo ngay cho bộ phận CNTT, bộ phận văn phòng tạm thời thu hồi quyền truy cập đối với hệ thống thông tin, dữ liệu, truy cập vật lý (nếu cần) và chuyển đơn vị có trách nhiệm thực hiện điều tra.

d) Sau khi có kết luận của cơ quan có thẩm quyền: Đối với trường hợp công chức vi phạm sẽ bị xử lý theo quy định; trường hợp không vi phạm đơn vị quản lý trực tiếp thông báo bộ phận CNTT và bộ phận văn phòng thực hiện khôi phục quyền truy cập.

3. Khi thay đổi vị trí công tác hoặc chấm dứt công việc

Khi công chức thay đổi vị trí công tác, điều động, biệt phái, nghỉ hưu, thôi việc, Ban TCCB/Phòng TCCB có trách nhiệm thông báo kịp thời cho bộ phận CNTT và bộ phận văn phòng để thực hiện điều chỉnh hoặc thu hồi quyền truy cập,

tài khoản, thiết bị, tài sản và các quyền liên quan theo quy định.

Điều 20. Bảo đảm an toàn thông tin đối với các đơn vị bên ngoài thực hiện cung cấp các dịch vụ

1. Trước khi thực hiện công việc

a) Đơn vị cung cấp dịch vụ thực hiện: Lập danh sách nhân sự tham gia hợp đồng; cung cấp hồ sơ nhân sự theo yêu cầu của hợp đồng và Bản cam kết bảo mật thông tin của các nhân sự này theo yêu cầu của hợp đồng; thực hiện đào tạo cho nhân sự và gửi báo cáo cho đơn vị quản lý hợp đồng sau khi được phổ biến quy định về an toàn, bảo mật thông tin. Đối với nhân sự được phân công thực hiện công việc liên quan đến trao đổi thông tin theo Điều ước quốc tế về Thuế, cần phải có lý lịch tư pháp.

b) Đơn vị quản lý hợp đồng có trách nhiệm kiểm tra hồ sơ, Bản cam kết bảo mật thông tin; phối hợp với đơn vị cung cấp dịch vụ và các đơn vị liên quan phổ biến quy định về an toàn, bảo mật thông tin cho nhân sự trước khi đề nghị cấp quyền truy cập.

c) Đối với các chuyên gia không nằm trong danh sách nhưng cần vào hỗ trợ hệ thống trong trường hợp khẩn cấp, đơn vị cung cấp dịch vụ phải có trách nhiệm đảm bảo an toàn thông tin với các cá nhân này.

2. Trong quá trình thực hiện hợp đồng

a) Đơn vị cung cấp dịch vụ có trách nhiệm quản lý nhân sự tham gia hợp đồng; kịp thời thông báo đơn vị quản lý hợp đồng khi có sự thay đổi về nhân sự, phạm vi công việc hoặc phát sinh yếu tố ảnh hưởng đến quyền truy cập.

b) Đơn vị quản lý hợp đồng có trách nhiệm phối hợp với bộ phận CNTT để đề nghị cấp mới, thay đổi, tạm dừng, thu hồi hoặc khôi phục quyền truy cập hệ thống. Bộ phận văn phòng đề nghị cấp mới, thay đổi, tạm dừng, thu hồi hoặc khôi phục quyền truy cập vật lý theo quy định khi có thay đổi về người lao động.

c) Định kỳ hằng năm hoặc khi có sự thay đổi, đơn vị cung cấp dịch vụ phối hợp với đơn vị quản lý hợp đồng tổ chức nhắc lại nghĩa vụ bảo mật và cập nhật kiến thức về an toàn, bảo mật thông tin cho các nhân sự tham gia hợp đồng.

d) Khi phát hiện hoặc tiếp nhận thông tin về việc nhân sự tham gia hợp đồng có dấu hiệu vi phạm quy định về an toàn, bảo mật thông tin, đơn vị cung cấp dịch vụ phải báo lại đơn vị quản lý hợp đồng. Đơn vị quản lý hợp đồng báo ngay cho: bộ phận CNTT để tạm thời thu hồi quyền truy cập hệ thống; bộ phận văn phòng thực hiện tạm thời thu hồi quyền truy cập vật lý; đồng thời báo cáo lãnh đạo đơn vị để xác minh, xử lý theo quy định. Trường hợp có dấu hiệu vi phạm pháp luật thì chuyển cơ quan có thẩm quyền để điều tra theo quy định.

đ) Sau khi có kết luận của cơ quan có thẩm quyền, nhân sự sẽ bị xử lý theo quy định. Trong trường hợp không vi phạm, đơn vị quản lý trực tiếp thông báo bộ phận CNTT và bộ phận Văn phòng thực hiện khôi phục quyền truy cập.

3. Khi hợp đồng hết hiệu lực

a) Đơn vị quản lý hợp đồng có trách nhiệm phối hợp với đơn vị cung cấp dịch vụ và các đơn vị liên quan thực hiện bàn giao, thu hồi hồ sơ, tài liệu, dữ liệu, tài khoản, thiết bị đã cấp cho nhân sự tham gia hợp đồng.

b) Đơn vị quản lý hợp đồng thông báo cho Văn phòng thực hiện thu hồi thẻ ra vào cho nhân sự tham gia hợp đồng.

c) Đơn vị quản lý hợp đồng thông báo cho bộ phận CNTT để thu hồi quyền truy cập hệ thống cho nhân sự tham gia hợp đồng.

d) Việc chấm dứt hoặc hết hiệu lực hợp đồng không làm chấm dứt nghĩa vụ bảo mật thông tin của tổ chức, nhà cung cấp dịch vụ và nhân sự tham gia hợp đồng theo quy định của hợp đồng và Bản cam kết bảo mật thông tin đã ký.

Chương V
BẢO ĐẢM AN NINH VẬT LÝ

Điều 21. Bảo đảm an ninh vật lý

1. Phân loại và quản lý các khu vực an ninh

a) Khu vực sân, đường nội bộ xung quanh tòa nhà: Các khu vực này được kiểm soát vào/ra bởi bộ phận bảo vệ cơ quan thuế; có hệ thống camera giám sát an ninh được duy trì ghi hình toàn bộ các hoạt động.

b) Khu vực công cộng và sử dụng chung bên trong tòa nhà gồm: Sảnh, hành lang các tầng; cầu thang máy và cầu thang bộ; tầng hầm (nếu có); căng tin; hội trường. Các khu vực này được kiểm soát an ninh vào/ra bằng thẻ từ hoặc được bộ phận lễ tân kiểm soát, tiếp đón tại sảnh.

c) Khu vực phục vụ (gồm các phòng làm việc của người lao động/phục vụ vệ sinh (phòng tạp vụ)): Được bố trí tại các phòng góc tại tòa nhà để tập kết các dụng cụ, thiết bị làm sạch, vệ sinh và nghỉ ngơi giữa giờ. Phòng Tạp vụ có khóa cửa, ngoài những người lao động/phục vụ vệ sinh được phép mở khóa để vào/ra, khu vực này còn được bộ phận kỹ thuật quản trị tòa nhà có quyền truy cập (vào/ra bằng chìa khóa dự phòng) để xử lý các vấn đề liên quan đến hệ thống thiết bị kỹ thuật tòa nhà có trong các phòng này khi có phát sinh.

d) Khu vực làm việc (phòng làm việc chung của các công chức): Các phòng làm việc đều có khóa cửa, các công chức khi ra vào phòng làm việc đều đóng/khóa cửa để đảm bảo không có người lạ vào phòng. Tất cả các công chức không thể

vào được các phòng làm việc khác, ngoại trừ những phòng/khu vực họ được phân công, bố trí làm việc. Sau khi hết giờ làm việc các phòng làm việc đều được khóa và chỉ có những người trong phòng mới có thể mở khóa để ra vào phòng. Nếu thời gian nghỉ kéo dài (ngày lễ, tết) ngoài việc khoá phòng, các cửa còn được niêm phong bảo mật theo quy định.

đ) Khu vực an ninh hạn chế (phòng điều hành thiết bị kỹ thuật tòa nhà, trạm biến áp, phòng đặt máy phát điện dự phòng, phòng kỹ thuật PCCC, phòng kiểm soát công nghệ thông tin, các phòng kỹ thuật điện/kỹ thuật mạng/kỹ thuật điều hòa; các phòng kho lưu trữ tài liệu của cơ quan thuế): Được đóng/khóa an toàn và chỉ có những người có nhiệm vụ (nhân viên kỹ thuật Văn phòng) mới được truy cập, mở cửa để vào thực hiện nhiệm vụ.

e) Khu vực an ninh cao (khu vực/phòng làm việc của Tổ chuyên trách trao đổi thông tin): Khu vực hoạt động, làm việc của TĐTT sẽ được bố trí riêng biệt, đảm bảo tính biệt lập và hạn chế tiếp cận đối với người không có nhiệm vụ, thẩm quyền. Khu vực này thiết lập chế độ kiểm soát truy cập bằng khóa điện tử hoặc thiết bị sinh trắc học được phân quyền truy cập cho người có thẩm quyền theo quy định và có camera giám sát theo dõi xung quanh khu vực kèm theo hệ thống cảnh báo qua loa kết nối với hệ thống giám sát hình ảnh đặt tại phòng giám sát hệ thống kỹ thuật tòa nhà.

2. Cấp và quản lý quyền truy cập vật lý

a) Nguyên tắc đặc quyền tối thiểu: Quyền truy cập vào các khu vực an ninh hạn chế và cao chỉ được cấp cho những cá nhân có công việc hợp lệ, được phê duyệt bằng văn bản bởi cấp có thẩm quyền.

b) Ghi nhận và rà soát: Toàn bộ quyền truy cập phải được phân quyền định danh cá nhân và lưu vết tự động. Định kỳ 06 tháng/lần rà soát lại danh sách quyền truy cập.

c) Thu hồi khẩn cấp: Kịp thời thu hồi quyền truy cập vật lý (thẻ từ, dấu vân tay, tài khoản) khi công chức thay đổi vị trí công tác, nghỉ việc, chấm dứt hợp đồng hoặc khi phát hiện nguy cơ an ninh.

3. Quản lý khách, nhà thầu và bên thứ ba

Khách, nhà thầu và các bên thứ ba khi vào các khu vực làm việc nội bộ, khu vực hạn chế hoặc khu vực an ninh cao phải tuân thủ:

a) Xác minh danh tính bằng giấy tờ tùy thân hợp pháp và đăng ký đầy đủ thông tin (họ tên, đơn vị, mục đích, thời gian).

b) Chỉ được di chuyển và tác nghiệp trong phạm vi được cấp phép.

c) Phải có công chức phụ trách của đơn vị đi kèm và giám sát trực tiếp trong

suốt quá trình làm việc tại khu vực hạn chế và an ninh cao.

d) Nhật ký ra vào của bên thứ ba phải được lưu trữ tập trung và bảo vệ an toàn để phục vụ công tác hậu kiểm.

4. Kiểm soát ra vào

Các đơn vị phải triển khai các biện pháp kỹ thuật kiểm soát ra vào phù hợp tại các đường biên để ngăn ngừa tuyệt đối truy cập trái phép:

a) Sử dụng thẻ nhận dạng (thẻ chức danh có dán ảnh) đối với toàn bộ công chức.

b) Triển khai hệ thống kiểm soát cửa tự động (Access Control) bằng thẻ từ, mã số hoặc công nghệ sinh trắc học (vân tay, khuôn mặt).

c) Đối với khu vực an ninh cao, bắt buộc áp dụng xác thực đa yếu tố vật lý (ví dụ: Kết hợp thẻ từ và sinh trắc học) và thiết kế hệ thống cửa phân tách chống bám đuôi (Anti-passback).

5. Giám sát an ninh vật lý và bảo vệ dữ liệu

a) Biện pháp giám sát: Kết hợp lực lượng nhân viên bảo vệ và bộ phận kỹ thuật theo dõi hệ thống camera giám sát (CCTV) hoạt động liên tục 24/7/365. Hệ thống CCTV phải bao quát được toàn bộ các lối ra vào, hành lang của khu vực hạn chế và an ninh cao.

b) Thời hạn lưu trữ dữ liệu: Nhật ký truy cập hệ thống cửa và dữ liệu ghi hình từ camera giám sát phải được lưu trữ an toàn, liên tục trong thời gian tối thiểu là 30 ngày (đối với khu vực thông thường) và 03 tháng (đối với khu vực an ninh cao).

c) Bảo vệ dữ liệu trực quan: Dữ liệu ghi hình camera phải được mã hóa, phân quyền truy cập. Không được bố trí góc quét của camera hướng trực tiếp vào màn hình máy tính, bàn làm việc, máy in, hoặc nơi có thể đọc được thông tin trên tài liệu giấy và thông tin nhạy cảm của người nộp thuế.

d) Quy định mặt bàn sạch và màn hình sạch (Clear Desk/ Clear Screen): Công chức phải khóa màn hình máy tính khi rời khỏi vị trí làm việc; không để lộ tài liệu chứa dữ liệu thuế trên mặt bàn khi hết giờ làm việc; toàn bộ tài liệu mật phải được lưu giữ trong tủ khóa.

6. Rà soát và tăng cường kiểm soát rủi ro

a) Các biện pháp kiểm soát truy cập vật lý phải được đánh giá, báo cáo định kỳ hàng năm hoặc ngay khi có thay đổi lớn về hạ tầng, nhân sự, tổ chức hoặc khi xảy ra sự cố an ninh thông tin.

b) Các biện pháp kiểm soát bổ sung (như bố trí thêm nhân sự giám sát kép, cô lập vùng mạng vật lý) phải được triển khai ngay lập tức khi kết quả đánh giá

rủi ro định kỳ chỉ ra các lỗ hổng hoặc mối đe dọa mới.

c) Định kỳ hàng năm hoặc đột xuất, đơn vị quản lý trụ sở tổ chức kiểm thử hệ thống an toàn thông tin vật lý của tòa nhà gồm:

- Kiểm thử về hệ thống thiết bị giám sát an ninh;
- Kiểm thử xâm nhập vật lý;
- Kiểm thử hệ thống báo động và phản ứng sự cố;
- Kiểm thử khả năng chịu lỗi và dự phòng.

Căn cứ kết quả kiểm thử để ghi nhận, báo cáo cấp có thẩm quyền và đề xuất phương án khắc phục.

7. Tổ chức triển khai

a) Đối với trụ sở Cơ quan Cục Thuế phải bảo đảm các điều kiện an toàn vật lý theo các khoản 1, 2, 3, 4, 5, 6 tại Điều này.

b) Đối với trụ sở Thuế tỉnh, thành phố và Thuế cơ sở:

- Căn cứ điều kiện thực tế về quy mô trụ sở, cơ sở vật chất, trang thiết bị kỹ thuật và nguồn lực được giao, Thủ trưởng đơn vị tổ chức triển khai công tác bảo đảm an ninh vật lý đối với trụ sở làm việc trên cơ sở tham chiếu các nội dung quy định của các khoản 1, 2, 3, 4, 5, 6 Điều này; ưu tiên áp dụng trước các biện pháp thiết yếu nhằm kiểm soát người, phương tiện và bảo vệ các khu vực làm việc, hồ sơ, tài liệu, hệ thống thông tin đặc biệt là các khu vực an ninh cao (nếu có);
- Đối với các yêu cầu kỹ thuật, công nghệ hoặc hạ tầng chưa đáp ứng điều kiện triển khai, đơn vị thực hiện các biện pháp quản lý, kiểm soát thay thế phù hợp, đồng thời xây dựng kế hoạch hoàn thiện cơ sở vật chất, trang thiết bị và hệ thống kỹ thuật theo lộ trình, bảo đảm từng bước đáp ứng các yêu cầu về an ninh vật lý theo quy định của Quy chế này.

Chương VI
QUẢN LÝ AN TOÀN THÔNG TIN

Điều 22. Xác định cấp độ an toàn hệ thống thông tin

Việc xác định, thẩm định, phê duyệt, điều chỉnh, bổ sung hồ sơ đề xuất cấp độ an toàn hệ thống thông tin được thực hiện theo quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ.

Điều 23. Quản lý tài sản

1. Thiết lập và duy trì hệ thống quản lý danh mục tài sản phần cứng

a) Lập danh sách tài sản phần cứng: Bộ phận CNTT lập danh sách thiết bị của người dùng cuối, thiết bị di động, thiết bị lưu trữ ngoài, máy in, máy scan,

thiết bị mạng, thiết bị bảo mật, máy chủ trong môi trường vật lý, ảo hóa và điện toán đám mây; bộ phận văn phòng lập danh sách các thiết bị OT/IoT và máy photocopy.

b) Danh sách tài sản phần cứng bao gồm các thông tin cơ bản sau: Tên tài sản, mã nhận diện serial number, đơn vị sản xuất, model, vị trí vật lý lắp đặt, vị trí lắp đặt trong hệ thống mạng, đơn vị/cá nhân chịu trách nhiệm quản lý tài sản, địa chỉ mạng IP (đối với thiết bị đặt địa chỉ IP tĩnh), hệ điều hành/firmware, thời gian hết bảo hành, thời gian ngừng hỗ trợ kỹ thuật của hãng, các tài khoản và vai trò được phép truy cập tài sản, mục đích sử dụng, tình trạng sử dụng. Bộ phận CNTT và bộ phận văn phòng thực hiện cập nhật khi có thay đổi và kiểm kê danh sách định kỳ 01 lần/năm.

2. Thiết lập và duy trì hệ thống quản lý danh mục tài sản phần mềm

a) Bộ phận CNTT lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần mềm hiện đang được cài đặt trên các tài sản phần cứng tại khoản 1 của Điều này.

b) Danh sách tài sản phần mềm bao gồm các thông tin sau: Tên tài sản, phiên bản (nếu có), nhà sản xuất, loại license, đơn vị/cá nhân chịu trách nhiệm quản lý/ vận hành tài sản, thời gian hết bảo hành, thời gian ngừng hỗ trợ kỹ thuật của hãng, mục đích sử dụng, tình trạng sử dụng, tài sản phần cứng đang cài đặt, các tài khoản được phép truy cập tài sản (nếu có). Bộ phận CNTT thực hiện cập nhật khi có thay đổi và kiểm kê danh sách định kỳ 01 lần/năm.

3. Thiết lập và duy trì hệ thống quản lý danh mục tài sản dữ liệu

a) Bộ phận CNTT lập danh sách các CSDL để theo dõi, cập nhật trạng thái.

b) Danh sách tài sản dữ liệu bao gồm các thông tin sau: Tên CSDL, tên hệ quản trị CSDL, phiên bản, nhà sản xuất, địa chỉ IP máy chủ, đơn vị/cá nhân chịu trách nhiệm quản lý tài sản, thời gian hết bảo hành, thời gian ngừng hỗ trợ kỹ thuật của hãng, mục đích sử dụng, tình trạng sử dụng, tài sản phần cứng đang cài đặt, các tài khoản và vai trò được phép truy cập tài sản, thông tin dữ liệu (dữ liệu cá nhân, dữ liệu NNT, dữ liệu công cộng, dữ liệu trao đổi thông tin, ...). Bộ phận CNTT thực hiện cập nhật khi có thay đổi và kiểm kê danh sách định kỳ tối thiểu 01 lần/năm.

4. Xử lý với các tài sản đã lỗi thời

a) Tài sản đã lỗi thời là tài sản không còn được nhà sản xuất hoặc nhà cung cấp hỗ trợ kỹ thuật, cập nhật phần mềm, bản vá bảo mật hoặc đã hết thời hạn bảo hành mà không còn khả năng gia hạn, dẫn đến không còn đáp ứng yêu cầu vận

hành hoặc an toàn thông tin.

b) Đối với tài sản đã lỗi thời, cơ quan thuế cần ưu tiên thay thế để đảm bảo tài sản luôn trong tình trạng bảo hành hoặc còn được hỗ trợ của hãng. Trường hợp, chưa thể thay thế, cơ quan thuế cần phải thể hiện rõ trong danh mục tài sản, đồng thời triển khai các biện pháp giảm thiểu rủi ro (với các thiết bị mà phần cứng còn được hãng bảo hành cần triển khai sao lưu dữ liệu, cấu hình hàng ngày; với các thiết bị có hệ điều hành, hệ quản trị CSDL không còn được hãng hỗ trợ, tăng cường vận hành hàng ngày để kịp thời phát hiện sự cố, không truy cập Internet)

Điều 24. Quản lý sự thay đổi

1. Quản lý sự thay đổi nhằm bảo đảm mọi thay đổi đối với hạ tầng CNTT, hạ tầng vật lý được thực hiện theo quy trình kiểm soát chặt chẽ, đánh giá đầy đủ rủi ro an toàn thông tin trước khi triển khai, nhằm duy trì tính bảo mật, toàn vẹn và sẵn sàng của dữ liệu.

2. Phân loại thay đổi bao gồm: Thay đổi tiêu chuẩn; thay đổi thông thường; thay đổi khẩn cấp.

3. Chủ trì thực hiện thay đổi:

a) Bộ phận CNTT là đơn vị chủ trì thực hiện các thay đổi đối với hạ tầng CNTT, bao gồm cả phòng máy chủ trong phạm vi cơ quan thuế.

b) Bộ phận văn phòng các đơn vị là đơn vị chủ trì thực hiện các thay đổi đối với hạ tầng vật lý.

4. Các đơn vị chủ trì xây dựng quy trình quản lý sự thay đổi, gồm các nội dung sau:

a) Lập yêu cầu thay đổi tối thiểu bao gồm:

- Mục tiêu và nội dung thay đổi;
- Hệ thống, dịch vụ hoặc quy trình bị ảnh hưởng;
- Lý do thực hiện thay đổi;
- Đề xuất thời gian triển khai;

b) Đánh giá tác động và rủi ro

- Tác động nghiệp vụ: Ảnh hưởng tới người nộp thuế; ảnh hưởng tới quy trình nghiệp vụ; ảnh hưởng tới chất lượng dịch vụ;
- Tác động đến hạ tầng CNTT/hạ tầng vật lý;
- Tác động an toàn thông tin: tính bí mật, tính toàn vẹn, tính sẵn sàng;
- Tác động đến tính liên tục dịch vụ: thời gian gián đoạn, khả năng phục hồi;
- Tác động pháp lý và tuân thủ: quy định pháp luật, quy định nội bộ, các quy

định khác.

c) Phê duyệt thay đổi: Người thực hiện phê duyệt thay đổi. Việc phê duyệt có thể phân cấp.

5. Kiểm thử thay đổi

a) Thay đổi phải được kiểm thử trước khi triển khai chính thức.

b) Việc kiểm thử phải được thực hiện trên môi trường độc lập với môi trường vận hành chính thức, trừ trường hợp không thể tách biệt về mặt kỹ thuật.

c) Dữ liệu phải thực hiện che giấu, ẩn danh hoặc giả lập dữ liệu.

d) Kết quả kiểm thử phải được ghi nhận và lưu trữ làm căn cứ phê duyệt triển khai.

đ) Các hệ thống không có môi trường kiểm thử cần phải sao lưu và có phương án khôi phục ban đầu.

6. Triển khai

a) Việc triển khai thay đổi phải được thực hiện theo kế hoạch đã được phê duyệt.

b) Trước khi triển khai phải xây dựng phương án sao lưu và phương án hoàn nguyên.

c) Đối với các thay đổi có nguy cơ ảnh hưởng đến hoạt động của hệ thống, phải có kế hoạch khôi phục dịch vụ trong trường hợp triển khai không thành công.

d) Sau khi triển khai phải thực hiện kiểm tra, xác nhận kết quả và giám sát hệ thống trong thời gian phù hợp.

7. Lưu trữ hồ sơ thay đổi:

a) Hồ sơ thay đổi phải được lưu trữ, theo dõi và phục vụ công tác kiểm tra, đánh giá, kiểm toán an toàn thông tin.

b) Định kỳ hàng năm rà soát quy trình quản lý sự thay đổi nhằm bảo đảm phù hợp với yêu cầu vận hành và an toàn thông tin.

Điều 25. Đánh giá rủi ro hệ thống thông tin và hạ tầng vật lý

1. Tất cả các hệ thống thông tin, hạ tầng vật lý của cơ quan thuế phải thực hiện đánh giá rủi ro hệ thống thông tin và hạ tầng vật lý trước khi đưa vào vận hành sử dụng hoặc khi có sự thay đổi hoặc khi xuất hiện mối đe dọa mới hoặc xảy ra sự cố an toàn thông tin.

2. Chủ trì quản lý rủi ro

a) Bộ phận CNTT là đơn vị chủ trì đánh giá rủi ro hệ thống tin.

b) Bộ phận Văn phòng các đơn vị là đơn vị chủ trì đánh giá rủi ro hạ tầng vật

lý.

3. Đơn vị chủ trì xây dựng quy trình đánh giá rủi ro gồm các bước sau:

a) Xác định danh mục tài sản, mức độ quan trọng và xác định chủ sở hữu đang quản lý đối với từng tài sản. Tài sản thông tin, hình ảnh và uy tín của tổ chức, phần mềm, phần cứng, tài sản vật lý khác, dịch vụ thuê ngoài, dịch vụ hỗ trợ nội bộ.

b) Nhận diện mối đe dọa, điểm yếu và kịch bản rủi ro: Xác định các mối đe dọa, khả năng xảy ra, điểm yếu các kịch bản rủi ro có khả năng tác động đến tài sản (rủi ro liên quan đến: vật lý, truy cập trái phép, thiết bị cá nhân, hạ tầng thông tin, bên thứ ba).

c) Đánh giá mức độ ảnh hưởng.

d) Đánh giá mức độ rủi ro.

đ) Xác định các biện pháp kiểm soát:

- Chấp nhận rủi ro;

- Giảm thiểu rủi ro;

- Tránh rủi ro;

- Chuyển giao rủi ro.

e) Dựa trên kết quả giám sát định kỳ việc triển khai các biện pháp kiểm soát, kết quả kiểm tra, tìm kiếm điểm yếu và các hoạt động rà soát khác, các đơn vị chủ quản tài sản phải cập nhật quy trình quản lý rủi ro và các kết quả đánh giá rủi ro tương ứng.

Điều 26. Đảm bảo hoạt động liên tục của nghiệp vụ

1. Lập kế hoạch duy trì hoạt động liên tục nhằm bảo đảm các hoạt động trọng yếu (các hoạt động có ảnh hưởng đến nghĩa vụ, trách nhiệm của người nộp thuế, các hoạt động trao đổi thông tin mang tính quốc tế) của cơ quan thuế được duy trì hoặc được khôi phục trong thời gian phù hợp khi xảy ra sự cố hoặc thảm họa.

2. Kế hoạch duy trì hoạt động liên tục phải được xây dựng trên cơ sở đánh giá rủi ro và đánh giá mức độ ảnh hưởng đối với hoạt động của cơ quan thuế, bao gồm các nội dung sau:

a) Xác định các kịch bản có khả năng gây gián đoạn hoạt động, bao gồm: không có địa điểm làm việc do thiên tai, hỏa hoạn, dịch bệnh, mất điện diện rộng; không đảm bảo hạ tầng kỹ thuật do tấn công mạng, tấn công mã độc, sự cố hạ tầng kỹ thuật, gián đoạn dịch vụ của nhà cung cấp.

b) Xây dựng phương án bảo đảm an toàn cho con người, tài sản, hệ thống

thông tin và thông tin, dữ liệu; bảo đảm tính bảo mật, toàn vẹn và khả dụng của thông tin, dữ liệu trong quá trình ứng phó, duy trì và khôi phục hoạt động; kiểm soát quyền truy cập, xác thực người dùng, giám sát và xử lý các nguy cơ mất an toàn, an ninh thông tin;

c) Đánh giá mức độ ảnh hưởng của từng kịch bản đối với các quy trình nghiệp vụ, hệ thống thông tin, hoạt động quản lý thuế, thu ngân sách nhà nước, trao đổi thông tin quốc tế và các hoạt động trọng yếu khác; xác định các hoạt động và hệ thống cần ưu tiên duy trì hoặc khôi phục.

d) Xây dựng kế hoạch duy trì hoạt động liên tục, bao gồm:

- Điều kiện và thẩm quyền kích hoạt kế hoạch duy trì hoạt động liên tục;

- Phương án bảo đảm an toàn cho con người, tài sản và thông tin, dữ liệu;

- Phương án duy trì hoạt động khi không thể sử dụng trụ sở làm việc;

- Phương án duy trì hoạt động các dịch vụ hạ tầng CNTT;

- Danh sách đầu mối liên hệ và các nhà cung cấp trọng yếu tham gia ứng cứu, khôi phục;

- Điều kiện, trình tự và thẩm quyền quyết định chuyển từ trạng thái ứng phó sự cố sang trạng thái vận hành bình thường.

đ) Đối với các quy trình nghiệp vụ phụ thuộc vào hệ thống thông tin, kế hoạch duy trì hoạt động liên tục phải xác định rõ việc phối hợp và kích hoạt kế hoạch khôi phục sau thảm họa để bảo đảm khôi phục hệ thống công nghệ thông tin phục vụ hoạt động nghiệp vụ.

3. Bộ phận CNTT/ bộ phận văn phòng có trách nhiệm xây dựng, duy trì, kiểm thử và cập nhật Kế hoạch khôi phục sau thảm họa đối với các hệ thống thuộc phạm vi quản lý, bảo đảm 01 lần/năm.

4. Đào tạo và diễn tập: Kế hoạch duy trì hoạt động liên tục phải được đơn vị nghiệp vụ chủ trì quy trình kiểm thử 01 lần/năm thông qua hình thức diễn tập mô phỏng hoặc diễn tập thực tế. Kết quả kiểm thử phải được lập thành báo cáo và lưu giữ theo quy định. Ban TCCB/phòng TCCB có trách nhiệm tổ chức đào tạo, phổ biến và nâng cao nhận thức về kế hoạch duy trì hoạt động liên tục cho công chức và người lao động có liên quan theo kế hoạch của Cục Thuế, đảm bảo 01 lần/năm. Đơn vị quản lý quy trình nghiệp vụ, Ban CĐS và các đơn vị có liên quan chịu trách nhiệm xây dựng nội dung chuyên môn, kịch bản diễn tập, quy mô tổ chức và phối hợp triển khai khi có kế hoạch và đề nghị của Ban TCCB.

Điều 27. Quản lý đơn vị cung cấp dịch vụ

1. Thiết lập danh mục các đơn vị cung cấp dịch vụ

a) Đơn vị quản lý hợp đồng lập danh mục các đơn vị cung cấp dịch vụ hoặc đơn vị có quyền truy cập hoặc có khả năng tiếp cận vào hệ thống thông tin của cơ quan thuế. Đơn vị cung cấp có thể bao gồm: đơn vị phát triển hoặc bảo trì phần mềm; nhà cung cấp hạ tầng CNTT, dịch vụ điện toán đám mây, đường truyền, trung tâm dữ liệu, dịch vụ giám sát an toàn thông tin; đơn vị bảo trì thiết bị CNTT, điều hòa, UPS, hệ thống phòng cháy chữa cháy, máy in, máy photocopy; đơn vị vệ sinh, bảo vệ, chuyển phát, đơn vị/cá nhân phiên dịch...

b) Danh mục đơn vị cung cấp dịch vụ bao gồm các thông tin sau: Tên nhà cung cấp, số hợp đồng cung cấp, thời hạn hợp đồng, dịch vụ hoặc sản phẩm cung cấp, phạm vi hệ thống được phép truy cập, loại dữ liệu được phép tiếp cận, đầu mối quản lý hợp đồng.

2. Trước khi ký kết hợp đồng hoặc cho phép đơn vị cung cấp dịch vụ truy cập vào hệ thống thông tin, đơn vị quản lý hợp đồng phải thực hiện đánh giá rủi ro an toàn thông tin đối với đơn vị cung cấp dịch vụ để xác định các biện pháp kiểm soát an toàn thông tin phù hợp. Việc đánh giá rủi ro, phân loại mức độ rủi ro và áp dụng các biện pháp kiểm soát an toàn thông tin.

3. Yêu cầu về an toàn thông tin với đơn vị cung cấp dịch vụ phải đáp ứng các nội dung sau:

a) Trách nhiệm bảo mật thông tin.

b) Quy định về quyền kiểm tra, giám sát và đánh giá của cơ quan thuế (nếu cần).

c) Thông báo ngay khi phát hiện sự cố an toàn thông tin hoặc nghi ngờ rò rỉ dữ liệu; các thay đổi có ảnh hưởng đến an toàn thông tin; các lỗ hổng bảo mật nghiêm trọng; các sự cố hoặc nghi ngờ sự cố an toàn thông tin; các thay đổi về nhân sự có quyền truy cập vào hệ thống của cơ quan thuế.

d) Nghĩa vụ phối hợp điều tra, xử lý và khắc phục sự cố.

đ) Yêu cầu về chất lượng dịch vụ.

e) Yêu cầu về duy trì hoạt động liên tục và khôi phục sau thảm họa (nếu có).

4. Quản lý quyền truy cập của đơn vị cung cấp dịch vụ

a) Việc cấp quyền truy cập cho đơn vị cung cấp dịch vụ phải được phê duyệt theo quy định.

b) Chỉ cấp quyền đúng phạm vi công việc, đúng thời gian và đúng hệ thống cần thiết.

c) Quyền truy cập phải được thu hồi ngay sau khi hoàn thành công việc hoặc khi hợp đồng chấm dứt hoặc khi có dấu hiệu vi phạm.

5. Giám sát và đánh giá đơn vị cung cấp dịch vụ

a) Đơn vị quản lý hợp đồng có trách nhiệm kiểm tra, giám sát việc tuân thủ các yêu cầu về an toàn thông tin của đơn vị cung cấp dịch vụ trong suốt quá trình thực hiện hợp đồng.

b) Đơn vị cung cấp dịch vụ báo cáo hoặc cung cấp tài liệu chứng minh việc tuân thủ các yêu cầu về an toàn thông tin, bao gồm các nội dung sau:

- Việc thực hiện các cam kết trong hợp đồng;

- Việc đáp ứng các mức chất lượng dịch vụ;

- Các sự cố an toàn thông tin phát sinh và việc thực hiện các yêu cầu khắc phục sự cố (nếu có);

- Kết quả kiểm tra hoặc đánh giá độc lập (nếu có);

- Việc thực hiện các yêu cầu khắc phục sau đánh giá (nếu có).

Điều 28. Quản lý ứng phó sự cố an toàn thông tin

1. Phân loại sự cố gồm: Sự cố an ninh hệ thống thông tin; sự cố an ninh vật lý.

2. Chủ trì ứng phó sự cố

a) Bộ phận CNTT là đơn vị chủ trì công tác ứng phó sự cố an ninh hệ thống thông tin.

b) Bộ phận văn phòng là đơn vị chủ trì công tác ứng phó sự cố an ninh vật lý.

3. Các đơn vị chủ trì ứng phó sự cố xây dựng chương trình ứng phó sự cố gồm các nội dung sau:

a) Thành lập đội ứng phó sự cố và chỉ định một công chức phụ trách chính và một công chức dự phòng để điều phối hoạt động ứng phó sự cố. Phân công rõ vị trí, vai trò, trách nhiệm của các thành viên tham gia ứng phó sự cố; định kỳ rà soát, cập nhật danh sách hàng năm hoặc khi có sự thay đổi.

b) Xây dựng danh sách đầu mối các đơn vị bên ngoài bao gồm các cơ quan chức năng, các đơn vị cung cấp dịch vụ (nếu có), các hãng công nghệ (nếu có) liên quan đến việc ứng phó sự cố. Định kỳ rà soát, cập nhật danh sách hàng năm hoặc khi có sự thay đổi.

c) Thiết lập và duy trì kênh liên lạc nhận thông tin cảnh báo về sự cố;

d) Thực hiện phân nhóm sự cố.

đ) Xây dựng quy trình ứng phó sự cố và được định kỳ rà soát, đánh giá hàng năm.

e) Đánh giá và báo cáo sau sự cố.

4. Thực hiện đánh giá sau sự cố:

a) Sau khi hoàn thành việc xử lý sự cố, đơn vị chủ trì phải tổ chức đánh giá, tổng kết và rút kinh nghiệm và có báo cáo gửi Tiểu ban An toàn thông tin.

b) Nội dung đánh giá tối thiểu bao gồm:

- Nguyên nhân phát sinh sự cố;
- Mức độ và phạm vi ảnh hưởng;
- Hiệu quả của hoạt động phát hiện, ứng phó và khắc phục;
- Các tồn tại, hạn chế trong quá trình xử lý;
- Các biện pháp khắc phục, phòng ngừa và cải tiến.

c) Hồ sơ sự cố, nhật ký xử lý, biên bản làm việc và các tài liệu liên quan phải được lưu giữ theo quy định.

5. Diễn tập ứng phó sự cố: Đơn vị chủ trì ứng phó sự cố xây dựng kế hoạch và tổ chức diễn tập ứng phó sự cố 01 lần/năm hoặc tham gia diễn tập với đơn vị cấp trên.

Chương VII
TỔ CHỨC THỰC HIỆN

Điều 29. Phổ biến, tuyên truyền, đào tạo, bồi dưỡng về an toàn thông tin

1. Tại Cục Thuế:

a) Ban TCCB chủ trì, phối hợp với các đơn vị có liên quan xây dựng kế hoạch đào tạo, bồi dưỡng về an toàn thông tin hằng năm theo kế hoạch đào tạo của Cục Thuế; tổ chức triển khai các khóa đào tạo, bồi dưỡng; quản lý, lưu giữ hồ sơ đào tạo theo quy định.

b) Ban CĐS/Ban QLTT/Văn phòng/Ban TCCB xây dựng nội dung chuyên môn, tài liệu đào tạo và phối hợp tổ chức đào tạo, bồi dưỡng về an toàn thông tin.

c) Văn phòng chủ trì, phối hợp với các đơn vị liên quan tổ chức tuyên truyền, phổ biến, nâng cao nhận thức về an toàn thông tin cho công chức và người lao động.

2. Tại Thuế tỉnh, thành phố:

a) Phòng TCCB chủ trì, phối hợp với các đơn vị liên quan xây dựng và tổ chức thực hiện kế hoạch đào tạo, bồi dưỡng về an toàn thông tin; quản lý, lưu giữ hồ sơ đào tạo theo quy định.

b) Phòng DLRR/Văn phòng/Phòng TCCB xây dựng nội dung chuyên môn, tài liệu đào tạo và phối hợp tổ chức đào tạo, bồi dưỡng về an toàn thông tin.

c) Văn phòng chủ trì, phối hợp với các đơn vị liên quan tổ chức tuyên truyền,

phổ biến, nâng cao nhận thức về an toàn thông tin cho công chức và người lao động.

Điều 30. Trách nhiệm của các cơ quan, đơn vị thuộc cơ quan thuế

1. Ban CĐS

a) Là đầu mối bảo đảm an toàn an ninh hệ thống thông tin.

b) Tổng hợp kế hoạch, báo cáo định kỳ, đột xuất về an toàn thông tin, trình Lãnh đạo Cục Thuế gửi các cơ quan quản lý về an toàn thông tin; xử lý các việc đột xuất về an toàn thông tin theo phân công của Cục Thuế.

c) Định kỳ hằng năm hoặc khi có thay đổi trong quy định của Nhà nước, chỉ đạo của cấp có thẩm quyền về an toàn thông tin: tổ chức rà soát, kiểm tra tính phù hợp của Quy chế này với các quy định của pháp luật về an toàn thông tin; kiểm tra tính đáp ứng của Quy chế này với yêu cầu thực tế của Cục Thuế; báo cáo Cục Thuế về việc sửa đổi, bổ sung Quy chế trong trường hợp cần thiết; lập hồ sơ lưu thông tin phản hồi của đối tượng áp dụng Quy chế về an toàn thông tin của Cục Thuế làm căn cứ xây dựng đề xuất cập nhật, bổ sung Quy chế.

d) Thực hiện sao lưu dữ liệu các hệ thống do Cục Thuế triển khai.

e) Công bố, cập nhật danh sách các trình duyệt web an toàn, danh sách địa chỉ trang thông tin điện tử được phép truy cập hàng năm hoặc khi có sự thay đổi.

g) Hướng dẫn việc xác định, thẩm định, phê duyệt, điều chỉnh, bổ sung hồ sơ đề xuất cấp độ an toàn hệ thống thông tin trong cơ quan thuế.

2. Các Ban/đơn vị thuộc Cơ quan Cục Thuế:

a) Văn phòng là đơn vị đảm bảo an ninh vật lý; quản lý vận hành hệ thống giám sát, an ninh, an toàn của trụ sở làm việc; hướng dẫn các đơn vị thuộc Cục Thuế triển khai công tác bảo đảm an ninh vật lý.

b) Ban QLTT là đầu mối quản lý, phân loại dữ liệu và các hoạt động xử lý, sử dụng dữ liệu; hướng dẫn các đơn vị thuộc Cục Thuế thực hiện quản lý, phân loại và xử lý, sử dụng dữ liệu theo quy định.

c) Ban TCCB là đầu mối quản lý an ninh thông tin con người; hướng dẫn các đơn vị thuộc Cục Thuế trong công tác bảo đảm an ninh thông tin con người.

d) Các Ban/đơn vị phối hợp triển khai và giám sát việc thực hiện Quy chế này trong phạm vi chức năng, nhiệm vụ được giao.

3. Thuế tỉnh, thành phố

a) Tổ chức triển khai thực hiện Quy chế này và các quy định của pháp luật, văn bản chỉ đạo và hướng dẫn của các cơ quan có thẩm quyền về an toàn thông tin trong phạm vi đơn vị; xây dựng kế hoạch, báo cáo định kỳ, đột xuất về an toàn

thông tin và gửi Ban CĐS tổng hợp, báo cáo Cục Thuế.

b) Ban hành quy định/ nội quy về an toàn thông tin của đơn vị phù hợp với trách nhiệm của đơn vị theo Quy chế này và các quy định của pháp luật về an toàn thông tin (nếu cần).

c) Giao Phòng DLRR là đầu mối triển khai công tác an toàn thông tin tại đơn vị.

4. Thuế cơ sở

a) Tổ chức tuyên truyền, triển khai thực hiện Quy chế này và các quy định của pháp luật, văn bản chỉ đạo và hướng dẫn của các cơ quan có thẩm quyền về an toàn thông tin trong phạm vi đơn vị; xây dựng kế hoạch, báo cáo định kỳ, đột xuất về an toàn thông tin và gửi Phòng DLRR.

b) Ban hành quy định/ nội quy về an toàn thông tin của đơn vị phù hợp với trách nhiệm của đơn vị theo Quy chế này và các quy định của pháp luật về an toàn thông tin (nếu cần).

c) Giao bộ phận công nghệ thông tin là đầu mối triển khai công tác an toàn thông tin tại đơn vị.

Điều 31. Trách nhiệm cá nhân thuộc cơ quan thuế

1. Thủ trưởng đơn vị thuộc đối tượng áp dụng của Quy chế này có trách nhiệm: phổ biến, quán triệt tới từng công chức, viên chức, người lao động của đơn vị thuộc phạm vi quản lý thực hiện nghiêm các quy định của pháp luật, quy định của Bộ Tài chính, quy định của cơ quan thuế về an toàn thông tin, bảo vệ dữ liệu cá nhân, bảo vệ bí mật nhà nước trên không gian mạng; thường xuyên kiểm tra việc thực hiện Quy chế này tại đơn vị; chịu trách nhiệm trước pháp luật và Lãnh đạo Cục Thuế về các vi phạm, thất thoát thông tin, dữ liệu mật thuộc phạm vi quản lý của đơn vị do không tổ chức, chỉ đạo, kiểm tra của đơn vị thực hiện đúng quy định hoặc để hệ thống thông tin thuộc phạm vi quản lý không đảm bảo các quy định về an toàn thông tin mạng.

2. Công chức, viên chức, người lao động thuộc cơ quan thuế có trách nhiệm: tuân thủ Quy chế; thông báo các vấn đề bất thường liên quan tới an toàn thông tin cho đơn vị chuyên trách an toàn hệ thống thông tin; chịu trách nhiệm trước pháp luật và Lãnh đạo đơn vị về các vi phạm, thất thoát dữ liệu mật của ngành Tài chính do không tuân thủ Quy chế.

3. Cá nhân vi phạm Quy chế tùy theo tính chất, mức độ của hành vi vi phạm sẽ bị xử lý hành chính, xử lý kỷ luật. Nếu gây thiệt hại về tài sản thì phải bồi thường theo quy định của pháp luật.

Điều 32. Kiểm tra, đánh giá an toàn thông tin

1. Cục Thuế xây dựng kế hoạch kiểm tra an toàn thông tin định kỳ hằng năm và đột xuất tại các đơn vị thuộc các cơ quan thuế. Trong đó, Ban CĐS tổ chức kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về an ninh hệ thống thông tin; Ban QLTT tổ chức kiểm tra đánh giá về bảo đảm chất lượng dữ liệu và các hoạt động xử lý, sử dụng dữ liệu; Văn phòng tổ chức kiểm tra, đánh giá việc tuân thủ quy định về đảm bảo an ninh vật lý, việc vận hành hệ thống giám sát, an ninh, an toàn của trụ sở làm việc; Ban TCCB tổ chức kiểm tra, đánh giá việc tuân thủ quy định an toàn, bảo mật thông tin đối với con người.

2. Thuế tỉnh, thành phố xây dựng kế hoạch kiểm tra an toàn thông tin định kỳ hằng năm và đột xuất tại các đơn vị thuộc cơ quan thuế tỉnh, thành phố, các Thuế cơ sở. Trong đó, Phòng DLRR tổ chức kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về an ninh hệ thống thông tin, an ninh dữ liệu, về bảo đảm chất lượng dữ liệu và các hoạt động xử lý, sử dụng dữ liệu; Văn phòng tổ chức kiểm tra, đánh giá việc tuân thủ quy định về đảm bảo an ninh vật lý, việc vận hành hệ thống giám sát, an ninh, an toàn của trụ sở làm việc; Phòng TCCB tổ chức kiểm tra, đánh giá việc tuân thủ quy định an toàn, bảo mật thông tin đối với con người.

Điều 33. Báo cáo an toàn thông tin

1. Ban TCCB, Văn phòng Cục Thuế, Ban QLTT (theo phân công tại Điều 30) lập báo cáo năm gửi Ban CĐS trước ngày 10 tháng 12. Ban CĐS tổng hợp, lập báo cáo gửi Tiểu ban An toàn thông tin, Cục Công nghệ thông tin và Chuyển đổi số trước ngày 20 tháng 12 hằng năm.

2. Thuế tỉnh, thành phố: Giao Phòng DLRR chủ trì, phối hợp với Văn phòng, Phòng TCCB thực hiện báo cáo định kỳ 6 tháng (trước ngày 10 tháng 6), báo cáo năm (trước ngày 10 tháng 12) gửi Cục Thuế (qua Ban CĐS).

Điều 34. Tổ chức thực hiện

1. Ban CĐS, Ban QLTT, Ban TCCB, Văn phòng Cục Thuế chịu trách nhiệm hướng dẫn, theo dõi, kiểm tra, đôn đốc việc thực hiện Quy chế này.

2. Trong quá trình thực hiện Quy chế trường phát sinh khó khăn, vướng mắc, các đơn vị, cá nhân gửi ý kiến về Ban CĐS để tổng hợp, báo cáo, đề xuất trình Lãnh đạo Cục Thuế xem xét, quyết định./.