UBND TỈNH TIỀN GIANG
SỞ TÀI CHÍNH

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

QUY CHẾ
Bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin tại Sở Tài chính tỉnh Tiền Giang

(Ban hành kèm theo Quyết định số 237/QĐ-STC ngày 26 tháng 8 năm 2022 của Sở Tài chính tỉnh Tiền Giang)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi, đối tượng áp dụng

1. Quy chế này quy định về nguyên tắc, trách nhiệm của công chức, viên chức và người lao động của Sở Tài chính trong việc quản lý, khai thác, sử dụng ứng dụng, phần mềm, thiết bị công nghệ thông tin nhằm bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin tại Sở Tài chính.

2. Các phòng thuộc Sở, đơn vị trực thuộc, công chức, viên chức, người lao động thuộc Sở và các cá nhân khác liên quan.

Điều 2. Nguyên tắc bảo đảm an toàn thông tin

1. Việc áp dụng Quy chế này nhằm phòng ngừa, ngăn chặn, xử lý và giảm các nguy cơ gây mất an toàn thông tin mạng và bảo đảm an ninh thông tin trong quá trình ứng dụng công nghệ thông tin trong hoạt động của Sở Tài chính.

2. Hoạt động an toàn thông tin mạng phải đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước, giữ vững ổn định chính trị, trật tự, an toàn xã hội và thúc đẩy phát triển kinh tế - xã hội; đảm bảo an toàn, an ninh thông tin trong hoạt động chuyên môn của Sở Tài chính.

3. Hoạt động an toàn thông tin mạng phải được thực hiện theo định kỳ, thường xuyên, liên tục, kịp thời và hiệu quả.

Điều 3. Các hành vi không được thực hiện

1. Các hành vi quy định tại Điều 7, Luật An toàn thông tin mạng năm 2015.

2. Lợi dụng mạng để truyền bá thông tin, quan điểm, thực hiện các hành vi gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, lợi ích quốc gia trên mạng; phá hoại khối đại đoàn kết toàn dân; tuyên truyền chiến tranh xâm lược, khủng bố; gây hận thù, mâu thuẫn giữa các dân tộc, sắc tộc, tôn giáo và bài ngoại.

3. Lợi dụng mạng để truyền bá trái phép tài liệu, hình ảnh, âm thanh hoặc dạng thông tin khác nhằm kích động bạo lực, dâm ô, đồi trụy, tội ác, tệ nạn xã hội, mê tín dị đoan, phá hoại thuần phong, mỹ tục của dân tộc; bôi nhọ, gây thù hận, xâm hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân.

Chương II
ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 4. Quản lý an toàn thông tin đối với người sử dụng

1. Khi tiếp nhận, tuyển dụng nhân sự mới, Văn phòng Sở có trách nhiệm phổ biến cho nhân sự mới các quy định về bảo đảm an toàn thông tin mạng tại cơ quan.

2. Thường xuyên phổ biến, quán triệt các quy định về an toàn thông tin mạng, nhằm nâng cao nhận thức về trách nhiệm bảo đảm an toàn thông tin mạng của từng cá nhân trong cơ quan.

3. Văn phòng Sở có trách nhiệm quản lý và thu hồi tài khoản, quyền truy cập các hệ thống thông tin và tất cả các tài sản liên quan tới hệ thống thông tin khi công chức, viên chức chuyển công tác, nghỉ việc, nghỉ theo chế độ.

Điều 5. Quản lý truy cập

1. Đối với công chức, viên chức và người lao động cơ quan phải có trách nhiệm

a) Bảo vệ bí mật thông tin tài khoản cá nhân hoặc tài khoản của cơ quan khi được phân công quản lý và sử dụng; đồng thời, phải thay đổi ngay mật khẩu tài khoản khi mới được cấp và tự chịu trách nhiệm trong việc quản lý, bảo vệ mật khẩu của tài khoản, không được cho người khác sử dụng tài khoản cá nhân hoặc của cơ quan.

b) Không đặt chế độ tự động ghi nhớ mật khẩu của các trình duyệt trong mọi trường hợp sử dụng.

c) Hệ thống mạng không dây (wifi) của cơ quan phải được cấp phát dãy IP riêng, không dùng chung dãy IP hệ thống mạng nội bộ và phải được đặt mật khẩu (password) khi truy cập. Thiết lập phương pháp hạn chế người dùng truy cập mạng không dây, giám sát và điều khiển truy cập mạng không dây.

d) Đặt mật khẩu đăng nhập, truy cập hệ thống thông tin có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặc biệt như !, @, #, $, %) và phải được thay đổi ít nhất 03 tháng/lần cho tất cả các tài khoản truy cập vào hệ thống máy chủ, thiết bị mạng, máy tính, các ứng dụng.

đ) Rà soát tối thiểu 03 tháng/lần các tài khoản đăng nhập, bảo đảm các tài khoản và quyền truy cập hệ thống được cấp phát đúng, đủ.

e) Chịu trách nhiệm về những thiệt hại do không tuân thủ các quy định về bảo vệ bí mật tài khoản dẫn đến thông tin cá nhân bị đánh cắp hay bị sửa đổi, các ứng dụng bị sử dụng mạo danh hay các hậu quả tiêu cực khác.

2. Đối với các hệ thống thông tin

a) Bảo đảm mỗi tài khoản của cơ quan, cá nhân truy cập vào hệ thống thông tin là duy nhất.

b) Các hệ thống thông tin cần giới hạn số lần đăng nhập sai liên tiếp vào hệ thống (từ 03 đến 05 lần). Hệ thống tự động khóa tài khoản trong một khoảng thời gian nhất định nếu liên tục đăng nhập sai vượt quá số lần quy định trước khi tiếp tục cho đăng nhập và có phương thức hỗ trợ cấp lại mật khẩu tài khoản.

Điều 6. Phòng, chống phần mềm độc hại

1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng, chống mã độc nhằm tăng cường bảo đảm an toàn, an ninh mạng và được thiết lập chế độ tự động cập nhật, tự động quét mã độc, virus...

2. Hệ điều hành, phần mềm cài đặt trên máy chủ, máy trạm phải được cập nhật bảng vá lỗ hổng bảo mật thường xuyên, kịp thời.

3. Công chức, viên chức và người lao động không được tự ý gỡ bỏ các phần mềm phòng, chống mã độc trên máy tính khi chưa có sự đồng ý của Lãnh đạo Sở.

4. Tất cả các máy trạm, máy chủ của cơ quan phải được cấu hình vô hiệu hóa tính năng tự động thực thi (autoplay) các tập tin trên các thiết bị lưu trữ di động.

5. Các máy tính xách tay, thiết bị di động (điện thoại thông minh, máy tính bảng...) trước khi kết nối vào mạng nội bộ của cơ quan phải bảo đảm đã được cài phần mềm phòng, chống mã độc.

6. Tất cả các tập tin, thư mục trên các thiết bị di động (USB, đĩa cứng di động…) phải được quét mã độc, virus trước khi sao chép vào máy tính sử dụng.

7. Máy chủ chỉ được dùng để cài đặt các phần mềm, dịch vụ dùng chung của cơ quan; không cài đặt phần mềm không rõ nguồn gốc, phần mềm phục vụ mục đích cá nhân và mục đích khác không phục vụ công việc.

8. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm mã độc, virus trên máy trạm như máy hoạt động chậm bất thường; cảnh báo từ phần mềm phòng, chống mã độc, tình trạng này lặp đi lặp lại nhiều lần và có dấu hiệu mất dữ liệu...người sử dụng phải tắt máy, ngắt kết nối từ máy tính đến mạng nội bộ, mạng Internet...và thông báo cho Văn phòng Sở để có hướng xử lý, khắc phục.

Điều 7. Bảo đảm an toàn trong xây dựng hệ thống thông tin

1. Các hoạt động liên quan đến xây dựng, thiết lập, quản lý, vận hành, nâng cấp mở rộng hệ thống thông tin phải thực hiện xác định cấp độ và phương án bảo đảm an toàn thông tin mạng theo quy định tại 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 và Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; phải tuân thủ Khung kiến trúc Chính quyền điện tử tỉnh Tiền Giang.

2. Văn phòng Sở phải tổ chức kiểm tra, đánh giá định kỳ về an toàn thông tin của các hệ thống thông tin đang quản lý.

Điều 8. Sao lưu dữ liệu dự phòng

1. Công chức, viên chức và người lao động khi lưu trữ, khai thác, trao đổi thông tin, dữ liệu phải bảo đảm tính toàn vẹn, tính tin cậy, tính sẵn sàng; phải áp dụng kỹ thuật mã hóa và thiết lập mật mã.

2. Phải thực hiện sao lưu dữ liệu dự phòng hàng ngày đối với các dữ liệu quan trọng và bảo đảm tính sẵn sàng cho việc sử dụng khi cần thiết.

Điều 9. Quản lý sự cố

1. Phân loại mức độ nghiêm trọng của các sự cố, bao gồm:

a) Thấp: sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan như máy trạm bị nhiễm phần mềm độc hại, virus; phần mềm hệ điều hành, các phần mềm ứng dụng cài đặt trên máy tính cá nhân phát sinh lỗi.

b) Trung bình: sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của cơ quan như hệ thống mạng của 01 phòng bị ngưng hoạt động, phần mềm độc hại, virus lây nhiễm tất cả các máy trạm trong 01 phòng.

c) Cao: sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và gây ảnh hưởng đến một trong các hoạt động chính của cơ quan như hệ thống quản lý văn bản và điều hành (văn phòng điện tử), một cửa điện tử bị ngưng hoạt động, một số thiết bị công nghệ thông tin quan trọng (thiết bị định tuyến, thiết bị tường lửa, máy chủ quản lý tập tin chung) bị hư hỏng.

d) Khẩn cấp: sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của cơ quan như toàn bộ hệ thống thiết bị công nghệ thông tin, hệ thống cung cấp điện ngừng hoạt động, hệ thống trang thông tin điện tử bị tin tặc (hacker) tấn công, xâm nhập, thay đổi nội dung...

2. Khi có sự cố hoặc nguy cơ mất an toàn thông tin mạng xảy ra như hệ thống hoạt động chậm bất thường, không truy cập được hệ thống, nội dung thông tin bị thay đổi không chủ động hoặc các dấu hiệu bất thường khác thì tiến hành quy trình ứng cứu sự cố an toàn thông tin mạng theo các bước sau:

a) Bước 1: nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc thẩm quyền cơ quan trực tiếp quản lý thì thực hiện tiếp Bước 2. Nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc Trung tâm Công nghệ thông tin và Truyền thông trực thuộc Sở Thông tin và Truyền thông quản lý (các hệ thống được triển khai tập trung tại Trung tâm Dữ liệu tỉnh) thì thực hiện tiếp Bước 3.

b) Bước 2: Văn phòng Sở tiến hành xử lý sự cố. Nếu sự cố được khắc phục thì lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố. Khi sự cố vượt quá khả năng xử lý, lập biên bản ghi nhận và thực hiện tiếp Bước 3.

c) Bước 3: báo sự cố đến Sở Thông tin và Truyền thông theo mẫu số 03 của Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ Thông tin và Truyền thông và thực hiện tiếp Bước 4.

d) Bước 4: phối hợp với Trung tâm Công nghệ thông tin và Truyền thông trực thuộc Sở Thông tin và Truyền thông và các cơ quan, tổ chức có liên quan để tiến hành khắc phục sự cố và thực hiện tiếp Bước 5.

đ) Bước 5: lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố theo mẫu số 04 của Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ Thông tin và Truyền thông và báo cáo bằng văn bản gửi về Sở Thông tin và Truyền thông.

3. Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục phải báo cáo ngay cho Sở Thông tin và Truyền thông

để được hướng dẫn, hỗ trợ.

Chương III
TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 10. Trách nhiệm của Lãnh đạo Sở Tài chính

1. Lãnh đạo, chỉ đạo công tác tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong công tác bảo đảm an toàn thông tin mạng của Sở Tài chính.

2. Phân công công chức chuyên trách bảo đảm an toàn thông tin mạng của cơ quan; tạo điều kiện để công chức phụ trách an toàn thông tin mạng được học tập, nâng cao trình độ về an toàn thông tin mạng; thường xuyên tổ chức quán triệt các quy định về an toàn thông tin mạng trong cơ quan.

3. Tạo điều kiện thuận lợi cho các cơ quan, đơn vị có liên quan tham gia khắc phục sự cố an toàn thông tin mạng kịp thời, nhanh chóng và đạt hiệu quả.

4. Phối hợp chặt chẽ với Công an tỉnh, Sở Thông tin và Truyền thông và các đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin mạng.

Điều 11. Trách nhiệm quản lý mạng nội bộ và đảm bảo an toàn hệ thống thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Sở Tài chính

1. Văn phòng Sở tham mưu Lãnh đạo Sở quản lý, vận hành, kiểm tra, giám sát và đảm bảo tính hiệu quả trong việc khai thác, sử dụng hệ thống thông tin, thiết bị công nghệ thông tin và đảm bảo an toàn thông tin mạng.

2. Hàng năm, căn cứ khả năng cân đối nguồn kinh phí và chế độ, tiêu chuẩn, định mức, Văn phòng Sở tham mưu Lãnh đạo Sở bố trí kinh phí triển khai thực hiện các nhiệm vụ về bảo đảm an toàn thông tin mạng.

Điều 12. Trách nhiệm của công chức, viên chức và người lao động

1. Trách nhiệm của công chức phụ trách an toàn thông tin mạng, công chức quản trị mạng

a) Chịu trách nhiệm bảo đảm an toàn thông tin mạng của cơ quan.

b) Tham mưu Lãnh đạo Sở ban hành các quy định, quy trình nội bộ và triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin mạng.

c) Thực hiện việc giám sát, đánh giá, báo cáo Lãnh đạo Sở các rủi ro mất an toàn thông tin mạng và mức độ nghiêm trọng của các rủi ro đó.

d) Phối hợp với các cơ quan, tổ chức và cá nhân có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn, an ninh thông tin.

2. Trách nhiệm của công chức, viên chức và người lao động

Công chức, viên chức và người lao động trong cơ quan phải:

a) Nghiêm chỉnh chấp hành các quy định tại Quy chế này và các quy định khác của pháp luật về an toàn thông tin, chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao.

b) Khi tham gia vận hành hệ thống thông tin, mạng máy tính của cơ quan, phải nghiêm chỉnh chấp hành chế độ bảo mật, an toàn, an ninh thông tin, đồng thời, chịu trách nhiệm đối với các thông tin mà mình cung cấp. Mỗi công chức, viên chức và người lao động phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp các thiết bị trên máy tính; không được vào các trang thông tin điện tử không rõ về nội dung; không tải và cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn; không nhấp chuột vào các đường dẫn lạ, không rõ về nội dung; không đưa các thông tin có nội dung "Mật", "Tối mật" và "Tuyệt mật" lên hệ thống máy tính có kết nối mạng Internet.

c) Trong trao đổi thông tin, dữ liệu phục vụ công việc, công chức, viên chức phải sử dụng hệ thống thông tin do cơ quan, đơn vị có thẩm quyền triển khai như hệ thống thư điện tử công vụ của tỉnh (https://mail.tiengiang.gov.vn) hoặc hệ thống thư điện tử của Bộ Tài chính (https://mail.mof.gov.vn); hệ thống quản lý văn bản và điều hành (văn phòng điện tử). Công chức, viên chức hạn chế sử dụng các trang mạng xã hội, các dịch vụ thư điện tử công cộng…để trao đổi thông tin quan trọng liên quan đến công việc chuyên môn của cơ quan.

d) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay Văn phòng Sở để kịp thời xử lý hoặc đề xuất xử lý và khắc phục sự cố.

Điều 13. Trách nhiệm của các tổ chức, cá nhân khác

Các tổ chức, cá nhân khi cần thiết có nhu cầu sử dụng các hệ thống thông tin do Sở Tài chính triển khai hoặc liên quan đến hoạt động ứng dụng công nghệ thông tin của Sở Tài chính phải tuân thủ Quy chế này và các quy định hiện hành của pháp luật có liên quan.

Điều 14. Xử lý vi phạm

Công chức, viên chức và người lao động có hành vi vi phạm Quy chế này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý theo quy định và pháp luật hiện hành.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 15. Tổ chức thực hiện

1. Giám đốc đơn vị trực thuộc Sở, Chánh Văn phòng Sở có trách nhiệm triển khai, hướng dẫn thực hiện các nội dung của Quy chế này đến toàn thể công chức, viên chức và người lao động của Sở.

2. Văn phòng Sở tham mưu Lãnh đạo Sở báo cáo về tình hình an toàn thông tin mạng theo hướng dẫn của Sở Thông tin và Truyền thông.

3. Công chức, viên chức và người lao động thuộc Sở có trách nhiệm thi hành Quy chế này.

Trong quá trình thực hiện, nếu có phát sinh khó khăn, vướng mắc cần sửa đổi, bổ sung, đề nghị công chức, viên chức và người lao động kịp thời báo cáo về Văn phòng Sở để tổng hợp trình Lãnh đạo Sở xem xét, điều chỉnh, bổ sung Quy chế cho phù hợp./.