ỦY BAN NHÂN DÂN THÀNH PHỐ HỒ CHÍ MINH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 03/2018/QĐ-UBND	*Thành phố Hồ Chí Minh, ngày 24 tháng 01 năm 2018*

QUYẾT ĐỊNH

Ban hành Quy chế về đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của các cơ quan nhà nước trên địa bàn Thành phố Hồ Chí Minh

ỦY BAN NHÂN DÂN THÀNH PHỐ HỒ CHÍ MINH

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19 tháng 6 năm 2015;

Căn cứ Luật Ban hành văn bản quy phạm pháp luật ngày 22 tháng 6 năm 2015;

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;

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

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Căn cứ Nghị định số 72/2013/NĐ-CP ngày 15 tháng 7 năm 2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng;

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

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 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 Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của 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;

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 31/TTr-STTTT ngày 27 tháng 12 năm 2017 và ý kiến thẩm định của Sở Tư pháp tại

Công văn số 10583/STP-VB ngày 20 tháng 10 năm 2017.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế về đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của các cơ quan nhà nước trên địa bàn Thành phố Hồ Chí Minh.

Điều 2. Quyết định này có hiệu lực kể từ ngày 05 tháng 02 năm 2018.

Điều 3. Chánh Văn phòng Ủy ban nhân dân thành phố, Giám đốc Công an thành phố, Giám đốc Sở Thông tin và Truyền thông, Thủ trưởng các Sở, ban, ngành, Chủ tịch Ủy ban nhân dân các quận, huyện và Thủ trưởng các cơ quan tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Nguyễn Thành Phong

ỦY BAN NHÂN DÂN THÀNH PHỐ HỒ CHÍ MINH	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY CHẾ

Về đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của các cơ quan nhà nước trên địa bàn Thành phố Hồ Chí Minh

(Ban hành kèm theo Quyết định số 03/2018/QĐ-UBND ngày 24 tháng 01 năm 2018 của Ủy ban nhân dân thành phố)

Chương I
QUY ĐỊNH CHUNG

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

1. Quy chế này quy định về công tác đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước, đơn vị sự nghiệp của Thành phố Hồ Chí Minh (sau đây gọi tắt là cơ quan).

2. Quy chế này được áp dụng đối với các các tổ chức, cá nhân liên quan đến an toàn, an ninh thông tin trong các cơ quan nhà nước, đơn vị sự nghiệp của Thành phố Hồ Chí Minh.

Điều 2. Mục đích, nguyên tắc đảm bảo 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 và đảm bảo an ninh thông tin trong quá trình ứng dụng công nghệ thông tin trong hoạt động của các cơ quan.

2. Các hoạt động ứng dụng công nghệ thông tin phải tuân theo nguyên tắc đảm bảo an toàn thông tin được quy định tại Điều 41, Nghị định 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước.

Điều 3. Giải thích từ ngữ

Trong Quy chế này, các từ ngữ dưới đây được hiểu như sau:

1. An toàn thông tin được quy định tại Khoản 1 Điều 3 Luật An toàn thông tin

mạng;

2. Hệ thống thông tin được quy định tại Khoản 3 Điều 3 Luật An toàn thông tin mạng;

3. Phần mềm độc hại được quy định tại Khoản 1 Điều 3 Luật An toàn thông tin mạng;

4. Nguy cơ mất an toàn thông tin là những nhân tố bên trong hoặc bên ngoài có khả năng ảnh hưởng tới trạng thái an toàn thông tin.

Chương II
QUY ĐỊNH ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 4. Về quản lý cán bộ, công chức, viên chức và người lao động

1. Các cơ quan phải xây dựng các yêu cầu, trách nhiệm đảm bảo an toàn thông tin đối với từng vị trí công việc. Sau khi tiếp nhận nhân sự mới, các cơ quan phải có trách nhiệm phổ biến cho nhân sự mới các quy định về đảm bảo an toàn thông tin tại cơ quan.

2. Các cơ quan phải thường xuyên tổ chức quán triệt các quy định về an toàn thông tin, nhằm nâng cao nhận thức về trách nhiệm đảm bảo an toàn thông tin của từng cá nhân trong cơ quan.

3. Các cơ quan phải xây dựng quy trình cấp mới, quản lý và thu hồi tài khoản (không hủy tài khoản), phân quyền truy cập các hệ thống thông tin và tất cả các tài sản liên quan tới hệ thống thông tin đối với các cá nhân do cơ quan quản lý.

Điều 5. Quản lý phòng máy chủ

1. Các thiết bị mạng quan trọng như tường lửa (firewall), thiết bị định tuyến (router), hệ thống máy chủ phải được đặt trong phòng máy chủ và có các biện pháp bảo vệ, ngăn chặn xâm nhập trái phép vào phòng máy chủ. đối với các điểm tập trung cable bên ngoài phòng máy chủ, phải có biện pháp bảo vệ, ngăn chặn xâm nhập trái phép.

2. Phòng máy chủ của các cơ quan là khu vực hạn chế tiếp cận và được lắp đặt hệ thống camera giám sát. Chỉ những người có trách nhiệm theo quy định của thủ trưởng cơ quan mới được phép vào phòng máy chủ.

3. Quá trình vào, ra phòng máy chủ phải được ghi nhận vào bản ghi nhật ký

quản lý phòng máy chủ.

4. Phòng máy chủ phải có hệ thống lưu điện đủ công suất và duy trì thời gian hoạt động của các máy chủ tối thiểu 15 phút khi có sự cố mất điện.

5. Phòng máy chủ phải có hệ thống giám sát nhiệt độ, độ ẩm để đảm bảo môi trường vận hành; hệ thống cảnh báo cháy, hệ thống chữa cháy tự động bằng khí, thiết bị phòng cháy chữa cháy khẩn cấp (CO2 khô); hệ thống cảnh báo hệ thống nguồn điện; hệ thống chống sét lan truyền. Tất cả cảnh báo này được gửi đến các cá nhân có trách nhiệm quản lý qua tin nhắn SMS hoặc thư điện tử. Cử cán bộ thường xuyên giám sát hệ thống thiết bị, hạ tầng của phòng máy chủ.

Điều 6. Phòng chống phần mềm độc hại

1. Tất cả các máy trạm, máy chủ phải được cài đặt phần mềm phòng chống phần mềm độc hại. Các phần mềm phòng chống phần mềm độc hại phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét khi sao chép, mở các tập tin.

2. Các cán bộ, công chức, viên chức và người lao động trong cơ quan phải được hướng dẫn về phòng chống phần mềm độc hại, các rủi ro do phần mềm độc hại gây ra; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm trên máy trạm khi chưa có sự đồng ý của người có thẩm quyền theo quy định của cơ quan.

3. Tất cả các máy tính của đơn vị phải được cấu hình nhằm vô hiệu hóa tính năng tự động thực thi (autoplay) các tập tin trên các thiết bị lưu trữ di động.

4. Các máy tính xách tay trước khi kết nối vào mạng nội bộ của cơ quan phải đảm bảo đã được cài chương trình phòng chống phần mềm độc hại và đã được kiểm duyệt về các phần mềm độc hại.

5. Tất cả các tập tin, thư mục phải được quét phần mềm độc hại trước khi sao chép, sử dụng.

6. Người sử dụng không được thiết lập chia sẻ dữ liệu trên máy tính của mình cho tất cả mọi người (nhóm phân quyền truy cập: everyone); không được chia sẻ với phân quyền tối đa (full control); nghiêm cấm lưu trữ dữ liệu cá nhân trên máy chủ hoặc các hệ thống lưu trữ dùng chung của đơn vị.

7. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy trạm như: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống phần mềm độc hại, tình trạng này lặp đi lặp lại nhiều lần, ở các vị trí khác nhau; quan trọng nhất là có dấu hiệu mất dữ liệu…, người sử dụng phải tắt máy

và báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý.

Điều 7. Sao lưu dữ liệu dự phòng

1. Các dữ liệu quan trọng của cơ quan phải được sao lưu, bao gồm: thông tin cấu hình của hệ thống mạng, máy chủ; phần mềm ứng dụng và cơ sở dữ liệu; bản ghi nhật ký hệ thống.

2. Các cơ quan phải lập kế hoạch và thực hiện sao lưu dữ liệu phù hợp với điều kiện của từng cơ quan, đảm bảo khả năng phục hồi dữ liệu khi có sự cố xảy ra.

Điều 8. Quản lý thiết bị tường lửa

1. Các hạ tầng công nghệ thông tin phải được trang bị thiết bị tường lửa và giám sát thường xuyên hoạt động của thiết bị này để ngăn chặn và phát hiện các xâm nhập trái phép vào mạng nội bộ.

2. Nhật ký hoạt động của thiết bị tường lửa phải được lưu giữ an toàn để phục vụ công tác khảo sát, điều tra khi có sự cố xảy ra.

Điều 9. Quản lý nhật ký trong quá trình vận hành các hệ thống thông tin

1. Các cơ quan phải thực hiện việc ghi nhật ký (log) trên các thiết bị mạng máy tính, phần mềm ứng dụng, hệ điều hành, cơ sở dữ liệu nhằm đảm bảo các sự kiện quan trọng xảy ra trên hệ thống được ghi nhận và lưu giữ.

2. Các bản ghi nhật ký này phải được bảo vệ an toàn nhằm phục vụ công tác kiểm tra, phân tích khi cần thiết.

3. Các sự kiện tối thiểu cần phải được ghi nhật ký gồm: quá trình đăng nhập hệ thống; tạo, cập nhật hoặc xóa dữ liệu; các hành vi xem, thiết lập cấu hình hệ thống; việc thiết lập các kết nối bất thường vào và ra hệ thống; thay đổi quyền truy cập hệ thống.

4. Thường xuyên thực hiện việc theo dõi bản ghi nhật ký của hệ thống và các sự kiện khác có liên quan để đánh giá, báo cáo các rủi ro và mức độ nghiêm trọng các rủi ro đó.

Điều 10. Quản lý truy cập

1. Các quy định về quản lý truy cập vào hệ thống thông tin, mạng máy tính, thiết bị, phần mềm ứng dụng của đơn vị phải được quy định chi tiết và tổ chức thực hiện nghiêm túc, phù hợp với các quy định của pháp luật về an toàn thông tin.

2. Mỗi tài khoản truy cập các hệ thống thông tin chỉ được giao cho một người

quản lý, sử dụng và chịu trách nhiệm chính về bảo mật an toàn thông tin truy cập tài khoản.

3. Mỗi cán bộ, công chức, viên chức và người lao động chỉ được phép truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình, có trách nhiệm bảo mật tài khoản truy cập thông tin.

4. Các hệ thống thông tin cần giới hạn số lần đăng nhập sai liên tiếp (không quá 10 lần) vào hệ thống. Hệ thống tự động khoá tài khoản trong một khoảng thời gian nhất định trước khi tiếp tục cho đăng nhập nếu liên tục đăng nhập sai vượt quá số lần quy định.

5. Tất cả máy trạm, máy chủ và các hệ thống thông tin phải được đặt mật khẩu truy cập và thiết lập chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng.

6. Khi thiết lập mạng không dây trong nội bộ đơn vị, phải đặt mật khẩu truy cập vào mạng không dây và chỉ cho phép truy cập Internet.

7. Các hệ thống thông tin phải thiết lập chế độ mật khẩu đăng nhập vào các hệ thống phải có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự số và ký tự đặc biệt như !, @, #, $, %) và phải được thay đổi ít nhất 3 tháng/lần. Các hệ thống thông tin phải thiết lập thời gian không truy cập của các tài khoản (trong 3 tháng), trong khoảng thời gian quy định này, các tài khoản không truy cập vào hệ thống sẽ bị khóa tài khoản.

8. Các hệ thống thông tin cần thiết lập thời hạn sử dụng của mật khẩu, sau 1 thời gian xác định mà người dùng không đổi mật khẩu thì sẽ tự động khóa tài khoản.

Điều 11. 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 tính trạm bị nhiễm phần mềm độc hại, 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 đoán hay đình trệ hoạt động chính của đơn vị như: hệ thống mạng của 1 (một) phòng, ban thuộc đơn vị bị ngưng hoạt động, phần mềm độc hại lây nhiễm tất cả các máy tính trạm trong 01 phòng, ban

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, hồ sơ cấp phép, một cửa điện tử của đơn vị bị ngưng hoạt động, một số thiết bị công nghệ thông tin quan trọng (bộ chuyển mạch trung tâm, 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 xảy ra, lãnh đạo đơn vị phải chỉ đạo kịp thời để khắc phục và hạn chế thiệt hại, báo cáo bằng văn bản cho cơ quan cấp trên trực tiếp quản lý và 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 của đơn vị, lãnh đạo đơn vị phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ.

Điều 12. Các hành vi bị nghiêm cấm

1. Tạo ra, cài đặt, phát tán phần mềm độc hại.

2. Xâm nhập, sửa đổi, xóa bỏ nội dung thông tin của cơ quan, cá nhân khác trái pháp luật.

3. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin.

4. Ngăn chặn việc truy nhập đến thông tin của cơ quan, cá nhân khác trên môi trường mạng, trừ trường hợp pháp luật cho phép.

5. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

6. Nghiêm cấm tự ý lắp đặt các thiết bị phát sóng Wifi (Access Point) vào mạng máy tính của cơ quan và lắp đặt các thiết bị tiếp sóng Wifi (Wireless card, wireless USB) trên máy tính có kết nối mạng nội bộ để truy cập mạng wifi ngoài khi chưa được phê duyệt của Lãnh đạo cơ quan.

7. Hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 13. Trách nhiệm của Ban chỉ đạo ứng dụng công nghệ thông tin của

Ủy ban nhân dân thành phố

Đảm nhiệm chức năng Ban chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng tại Thành phố Hồ Chí Minh và có trách nhiệm, quyền hạn thực hiện theo quy định tại Điều 5, Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ về ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.

Điều 14. Trách nhiệm của các cơ quan, đơn vị

1. Các cơ quan, đơn vị có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước Ủy ban nhân dân thành phố trong công tác đảm bảo an toàn thông tin của đơn vị mình.

2. Phân công một lãnh đạo đơn vị chịu trách nhiệm chỉ đạo bộ phận hoặc cán bộ chuyên trách thực hiện các công việc nhằm đảm bảo an toàn thông tin cho đơn vị.

3. Phân công một bộ phận hoặc cán bộ chuyên trách đảm bảo an toàn thông tin của đơn vị; tạo điều kiện để các cán bộ phụ trách an toàn thông tin được học tập, nâng cao trình độ về an toàn thông tin.

4. Xây dựng quy định, quy trình nội bộ về đảm bảo an toàn thông tin phù hợp với Quy chế này và các quy định của pháp luật.

5. Các cơ quan, đơn vị có trách nhiệm thực hiện xác định cấp độ an toàn thông tin và đảm bảo an toàn cho hệ thống thông tin của đơn vị đang quản lý theo quy định tại Luật An toàn thông tin mạng, 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 hướng dẫn tại Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của 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.

6. Có nghĩa vụ phải tham gia mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia và được quy định chi tiết về trách nhiệm, quyền hạn tại Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 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.

7. Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố xảy ra một cách kịp thời, nhanh chóng và đạt hiệu quả.

8. Phối hợp chặt chẽ với Công an thành phố trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn, an ninh thông tin.

9. Định kỳ mỗi 6 tháng, các cơ quan lập báo cáo về tình hình an toàn thông tin và gửi về Sở Thông tin và Truyền thông (theo hướng dẫn của Sở Thông tin và Truyền thông).

Điều 15. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các cơ quan

1. Trách nhiệm của cán bộ, công chức, viên chức phụ trách an toàn thông tin:

a) Chịu trách nhiệm đảm bảo an toàn thông tin của đơn vị;

b) Tham mưu lãnh đạo cơ quan ban hành các quy định, quy trình nội bộ, triển khai các giải pháp kỹ thuật đảm bảo an toàn thông tin;

c) Thực hiện việc giám sát, đánh giá, báo cáo thủ trưởng cơ quan các rủi ro mất an toàn thông tin và mức độ nghiêm trọng của các rủi ro đó;

d) Phối hợp với các cá nhân, đơn vị 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 cán bộ, công chức, viên chức và người lao động trong các cơ quan, đơn vị:

a) Nghiêm túc chấp hành các quy định, quy trình nội bộ, Quy chế này và các quy định khác của pháp luật về an toàn thông tin. Chịu trách nhiệm đảm bảo an toàn thông tin trong phạm vi trách nhiệm và quyền hạn được giao;

b) Khi tham gia vận hành 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 cán bộ, 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 cho phép bất cứ hành vi nào gây tổn hại đến dịch vụ, gây hư hỏng thiết bị mạng; không cung cấp thông tin không trung thực để công bố trên mạng; sử dụng mạng để thâm nhập vào các mạng máy tính khi chưa được phép; 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) Mỗi cán bộ, công chức, viên chức và người lao động không sử dụng các trang mạng xã hội, các dịch vụ thư điện tử công cộng (không phải hệ thống thư điện tử của thành phố) để trao đổi thông tin liên quan đến công việc chuyên môn của cơ quan;

d) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin phải báo cáo ngay với cấp trên và bộ phận chuyên trách công nghệ thông tin của đơn vị để kịp thời ngăn chặn và xử lý;

e) Tham gia các chương trình đào tạo, hội nghị về an toàn an ninh thông tin do cơ quan hoặc Sở Thông tin và Truyền thông tổ chức.

Điều 16. Trách nhiệm của Sở Thông tin và Truyền thông

1. Tham mưu Ủy ban nhân dân thành phố về công tác đảm bảo an toàn, an ninh thông tin trên địa bàn thành phố và chịu trách nhiệm trước Ủy ban nhân dân thành phố trong việc đảm bảo an toàn an ninh cho các hệ thống thông tin của thành phố.

2. Thực hiện thủ tục xác định cấp độ an toàn thông tin và đảm bảo an toàn cho các hệ thống thông tin dùng chung của thành phố theo quy định của Luật An toàn thông tin mạng, 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 hướng dẫn tại Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của 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.

3. Hằng năm xây dựng kế hoạch triển khai công tác đảm bảo an toàn thông tin phục vụ cho việc vận hành các hệ thống thông tin được Ủy ban nhân dân thành phố giao quản lý.

4. Chủ trì, phối hợp với Công an thành phố và các cơ quan, đơn vị liên quan tổ chức kiểm tra theo định kỳ hoặc đột xuất; kịp thời phát hiện và xử lý theo quy định của pháp luật đối với các cơ quan, tổ chức, cá nhân có các dấu hiệu, hành vi vi phạm an toàn, an ninh thông tin trên địa bàn thành phố.

5. Hằng năm xây dựng và triển khai các chương trình đào tạo chuyên sâu về an toàn, an ninh thông tin cho lực lượng đảm bảo an toàn, an ninh thông tin của các cơ quan, đơn vị.

6. Tổ chức các hội nghị, hội thảo chuyên đề và tuyên truyền về an toàn, an ninh thông tin trong công tác quản lý Nhà nước trên địa bàn thành phố.

7. Tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin.

8. Hướng dẫn, giám sát các cơ quan, đơn vị trên địa bàn thành phố xây dựng quy chế nội bộ và thực hiện việc đảm bảo an toàn, an ninh cho hệ thống thông tin theo quy định của Nhà nước.

9. Tổng hợp và báo cáo về tình hình an toàn, an ninh thông tin theo định kỳ cho Bộ Thông tin và Truyền thông, Ủy ban nhân dân thành phố và các cơ quan, đơn vị có liên quan.

Điều 17. Trách nhiệm của Công an thành phố

1. Chủ trì, phối hợp với Sở Thông tin và Truyền thông và các cơ quan, đơn vị có liên quan xây dựng kế hoạch và kiểm soát, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm sử dụng hệ thống thông tin gây hại đến an toàn, an ninh thông tin trong cơ quan nhà nước.

2. Phối hợp với các cơ quan chức năng kiểm tra, đánh giá, đề xuất biện pháp đảm bảo an toàn, an ninh thông tin.

3. Tăng cường công tác phối hợp các cơ quan, ban, ngành của thành phố tuyên truyền, phổ biến pháp luật về xử lý tội phạm xâm phạm an toàn, an ninh thông tin; hướng dẫn thực hiện và kiểm tra việc thi hành Quy chế bảo vệ bí mật Nhà nước trên địa bàn thành phố Hồ Chí Minh trong việc đảm bảo an toàn, an ninh thông tin.

4. Điều tra và đề xuất xử lý các trường hợp vi phạm pháp luật về an toàn, an ninh thông tin theo thẩm quyền.

5. Thực hiện nhiệm vụ bảo vệ an toàn các công trình quan trọng về an ninh quốc gia trên lĩnh vực công nghệ thông tin.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 18. Khen thưởng và xử lý vi phạm

1. Hàng năm, Sở Thông tin và Truyền thông dựa trên các điều tra, báo cáo công tác an toàn, an ninh thông tin của các cơ quan, đơn vị để xác lập bảng xếp hạng an toàn, an ninh thông tin, trên cơ sở đó đề xuất Ủy ban nhân dân thành phố xem xét khen thưởng theo quy định hiện hành.

2. Các cơ quan, đơn vị có hành vi vi phạm Quy chế này tùy theo tính chất, mức

độ vi phạm mà bị xử lý theo quy định của pháp luật hiện hành.

Điều 19. Thủ trưởng các sở, ban, ngành thành phố, Chủ tịch Ủy ban nhân dân các quận, huyện chịu trách nhiệm tổ chức triển khai thực hiện Quy chế tại đơn vị mình.

Điều 20. Sở Kế hoạch và Đầu tư, Sở Tài chính phối hợp Sở Thông tin và Truyền thông ưu tiên bố trí kinh phí thực hiện các nhiệm vụ đảm bảo an toàn thông tin của thành phố.

Điều 21. Trong quá trình thực hiện, nếu có những vấn đề cần sửa đổi, bổ sung, đề nghị các đơn vị gửi về Sở Thông tin và Truyền thông để tổng hợp, báo cáo Ủy ban nhân dân thành phố xem xét, quyết định./.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Nguyễn Thành Phong