ỦY BAN NHÂN DÂN HUYỆN BÌNH CHÁNH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 6469/QĐ-UBND	*Bình Chánh, ngày 17 tháng 8 năm 2022*

QUYẾT ĐỊNH

Ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của các cơ quan, đơn vị quản lý nhà nước huyện Bình Chánh

ỦY BAN NHÂN DÂN HUYỆN BÌNH CHÁNH

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19 tháng 6 năm 2015; Luật sửa đổi, bổ sung một số điều của Luật Tổ chức chính phủ và Luật Tổ chức Chính quyền địa phương ngày 22 tháng 11 năm 2019;

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 Luật An ninh mạng ngày 12 tháng 6 năm 2018;

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 Nghị định số 130/2018/NĐ-CP ngày 27 tháng 9 năm 2018 của Chính phủ về Quy định chi tiết thi hành Luật Giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số;

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;

Căn cứ Quyết định số 03/2018/QĐ-UBND ngày 24 tháng 01 năm 2018 của UBND Thành phố 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;

Căn cứ Tờ trình số 59/TTr-TTDL.TTDL ngày 10 tháng 8 năm 2022 của Trung tâm Dữ liệu và ứng dụng công nghệ thông tin huyện Bình Chánh,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của các cơ quan, đơn vị quản lý nhà nước huyện Bình Chánh.

Điều 2. Quyết định này có hiệu lực kể từ ngày ký.

Điều 3. Chánh Văn phòng Hội đồng nhân dân và Ủy ban nhân dân Huyện, Trưởng Công an Huyện, Trưởng phòng Tài chính kế hoạch, Thủ trưởng các cơ quan, đơn vị thuộc Huyện, Chủ tịch Ủy ban nhân dân xã, thị trấn và các cơ quan, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- TTUB: CT, các PCT;
- TT.DL&UDCNTT;
- VPUB: CVP, Các PVP;
- Lưu: VT - Tin học.

TM. ỦY BAN NHÂN DÂN
Q. CHỦ TỊCH

Phạm Văn Lũy

ỦY BAN NHÂN DÂN HUYỆN BÌNH CHÁNH	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY CHẾ

Đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của các cơ quan, đơn vị quản lý nhà nước huyện Bình Chánh

(Ban hành kèm theo Quyết định số 6469 /QĐ-UBND ngày 17 tháng 8 năm 2022 của Ủy ban nhân dân huyện Bình Chánh)

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 an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của các cơ quan nhà nước, đơn vị sự nghiệp của huyện Bình Chánh (sau đây gọi tắt là cơ quan).

2. Quy chế này được áp dụng đối với 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 huyện Bình Chánh.

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, chuyển đổi số trong hoạt động của các cơ quan.

2. Các hoạt động ứng dụng công nghệ thông tin, chuyển đổi số 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 là sự bảo vệ thông tin và hệ thống thông tin tránh bị truy cập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin;

2. Hệ thống thông tin là tập hợp thiết bị phần cứng, phần mềm và cơ sở 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 như: Hệ thống mạng nội bộ, hệ thống văn phòng điện tử, thư điện tử, trang thông tin điện tử...;

3. 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.

4. Phần mềm độc hại là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hoặc toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

5. Chữ ký số là một dạng chữ ký điện tử được tạo ra bằng sự biến đổi một thông điệp dữ liệu sử dụng hệ thống mật mã không đối xứng, theo đó, người có được thông điệp dữ liệu ban đầu và khóa công khai của người ký có thể xác định được chính xác;

Chữ ký số được phân loại tương ứng với chứng thư số, gồm: "chữ ký số cá nhân", "chữ ký số cơ quan, tổ chức", "chữ ký chuyên dùng", "chữ ký số chuyên dùng chính phủ", "chữ ký số công cộng", "chữ ký số nước ngoài".

6. Thiết bị lưu khóa bí mật là thiết bị vật lý chứa chứng thư số và khóa bí mật tương ứng với chứng thư số được cấp cho thuê bao; bao gồm các dạng thiết bị sau: etoken (thiết bị dạng thẻ USB), smartcard (thẻ thông minh), SIM PKI (thẻ SIM điện thoại), HSM (thiết bị ký số chuyên dụng cho tổ chức, từ viết tắt của Hardware Security Module).

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 cáp kết nối, đường truyền (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.

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 có bản quyền. 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 ngắt kết nối dây mạng, thiết bị mạng, ghi nhận (quay phim, chụp ảnh) các tình trạng, mã lỗi, 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 cài đặt thời gian lưu trữ tối đa, lưu giữ an toàn để phục vụ công tác khảo sát, điều tra khi có sự cố xảy ra.

Điều 9. 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 03 tháng/01 lần (hiệu lực sử dụng mật khẩu tối đa 03 tháng).

8. Chữ ký số phải được đảm bảo an toàn theo quy định tại Điều 9 và khoản 3 Điều 8 của Nghị định 130/2018/NĐ-CP như sau:

a) Chữ ký số được tạo ra trong thời gian chứng thư số có hiệu lực và kiểm tra được bằng khóa công khai ghi trên chứng thư số đó.

b) Chữ ký số được tạo ra bằng việc sử dụng khóa bí mật tương ứng với khóa công khai ghi trên chứng thư số do tổ chức cung cấp dịch vụ chứng thực chữ ký số hoạt động hợp pháp tại Việt Nam cung cấp hoặc chứng thư số nước ngoài được Bộ Thông tin và Truyền thông cấp giấy phép sử dụng tại Việt Nam.

c) Khóa bí mật chỉ thuộc sự kiểm soát của người ký tại thời điểm ký.

Điều 10. Các hành vi bị nghiêm cấm

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

2. Các hành vi can thiệp, điều chỉnh, xóa nhật ký hoạt động của thiết bị máy tính, thiết bị mạng, tường lửa khi chưa có ý kiến của thủ trưởng đơn vị.

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

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

5. 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.

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

7. 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.

8. 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 11. 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 huyện Bình Chánh 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. 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.

6. Đảm bảo giá trị pháp lý của chữ ký số được công nhận theo Điều 24 Luật Giao dịch điện tử năm 2005, Điều 8 Nghị định số 130/2018/NĐ-CP của

Chính phủ quy định chi tiết thi hành Luật giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số và các quy định của pháp luật trong lĩnh vực mà chữ ký số được áp dụng.

Điều 12. 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) Quản lý, sử dụng thiết bị lưu khóa bí mật và mật khẩu khóa bí mật, được cấp tương ứng với chứng thư số cho các hoạt động ký số văn bản điện tử trên hệ thống quản lý văn bản và điều hành điện tử; hồ sơ, chứng nhận điện tử trong các thủ tục hành chính công trực tuyến, dịch vụ công trực tuyến; trong các giao dịch điện tử khác theo quy định của pháp luật.

Điều 13. Trách nhiệm của Văn phòng Hội đồng nhân dân và Ủy ban nhân dân huyện Bình Chánh

1. Phối hợp Trung tâm dữ liệu và Ứng dụng công nghệ thông tin Huyện tham mưu Ủy ban nhân dân huyện Bình Chánh về công tác đảm bảo an toàn, an ninh thông tin tại các cơ quan và chịu trách nhiệm trước Ủy ban nhân dân huyện Bình Chánh trong việc đảm bảo an toàn an ninh cho các hệ thống thông tin của Huyện.

2. Phối hợp Trung tâm dữ liệu và Ứng dụng công nghệ thông tin Huyện 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.

3. Chủ trì, phối hợp với các cơ 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 tại Ủy ban nhân dân huyện Bình Chánh.

4. 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.

5. Trách nhiệm của cán bộ, công 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.

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

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 Huyện 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 Sở Thông tin và Truyền thông (theo hướng dẫn của Sở Thông tin

và Truyền thông), Ủy ban nhân dân huyện Bình Chánh và các cơ quan, đơn vị có liên quan.

Điều 14. Trách nhiệm của Công an Huyện

1. Phối hợp các phòng nghiệp vụ Công an Thành phố tham mưu Ủy ban nhân dân huyện Bình Chánh chỉ đạo các cơ quan, phòng, ban, tổ chức, đoàn thể chính trị Huyện triển khai tăng cường công tác bảo đảm an ninh, an toàn thông tin trên các thiết bị, hệ thống, phần mềm theo hướng dẫn của Công an Thành phố.

2. Tăng cường công tác phối hợp các cơ quan, ban, ngành của Huyện 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 huyện trong việc đảm bảo an toàn, an ninh thông tin.

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

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 15. Khen thưởng và xử lý vi phạm

1. Hàng năm, Văn phòng Hội đồng nhân dân và Ủy ban nhân dân huyện Bình Chánh 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 huyện Bình Chánh 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 16. Thủ trưởng các phòng, ban, đơn vị thuộc Huyện, Chủ tịch Ủy ban nhân dân xã, thị trấn chịu trách nhiệm tổ chức triển khai thực hiện Quy chế tại đơn vị mình.

Điều 17. Phòng Tài chính kế hoạch phối hợp Văn phòng Hội đồng nhân dân và Ủy ban nhân dân huyện Bình Chánh ưu tiên bố trí kinh phí thực hiện các nhiệm vụ đảm bảo an toàn thông tin của Huyện.

Điều 18. Trong quá trình thực hiện, nếu có những vấn đề cần sửa đổi, bổ sung, đề nghị các đơn vị gửi về Văn phòng Hội đồng nhân dân và Ủy ban nhân dân Huyện để tổng hợp, báo cáo Ủy ban nhân dân huyện Bình Chánh xem xét, quyết định./.