ỦY BAN NHÂN DÂN **HUYỆN NHÀ BÈ**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 1316 /QĐ-UBND	*Nhà Bè, ngày 10 tháng 7 năm 2024*

QUYẾT ĐỊNH
Về ban hành Quy chế đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin tại Ủy ban nhân dân Huyện và các xã, thị trấn huyện Nhà Bè

CHỦ TỊCH ỦY BAN NHÂN DÂN HUYỆN NHÀ BÈ

Căn cứ Luật Tổ chức Chính quyền địa phương ngày 19 tháng 6 năm 2015 và 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 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 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 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 Ủy ban nhân dân Thành phố về 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;

Xét đề nghị của Trưởng Phòng Văn hóa và Thông tin Huyện tại Tờ trình số 434 /TTr-VHTT ngày 05 tháng 7 năm 2024.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này là Quy chế đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin tại Ủy ban nhân dân Huyện và các xã, thị trấn huyện Nhà Bè

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, Thủ trưởng các cơ quan, đơn vị và Chủ tịch Ủy ban nhân dân các xã, thị trấn chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Sở Thông tin và Truyền thông Thành phố;
- Thường trực Huyện ủy;
- Thường trực HĐND;
- UBND Huyện: CT, các PCT;
- Lưu: VT.

CHỦ TỊCH

Triệu Đỗ Hồng Phước

ỦY BAN NHÂN DÂN HUYỆN NHÀ BÈ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc Lập - Tự Do - Hạnh phúc

QUY CHẾ

Đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin tại Ủy ban nhân dân Huyện và các xã, thị trấn huyện Nhà Bè

(kèm theo Quyết định số 1316/QĐ-UBND ngày 10 tháng 7 năm 2024 của Chủ tịch Ủy ban nhân dân huyện Nhà Bè)

Chương I

QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

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 bao gồm: công tác quản lý vận hành ứng dụng, kết nối mạng, trao đổi, chia sẻ, sử dụng, khai thác các cơ sở dữ liệu chuyên ngành trong hoạt động của các cơ quan nhà nước trên địa bàn huyện Nhà Bè.

Điều 2. Đối tượng áp dụng

1. Quy chế này áp dụng đối với các cơ quan, đơn vị bao gồm: các phòng, ban chuyên môn thuộc huyện; Ủy ban nhân dân các xã, thị trấn và các cơ quan, đơn vị có liên quan (sau đây gọi tắt là cơ quan).

2. Cán bộ, công chức, viên chức, người lao động đang làm việc tại các cơ quan theo khoản 1 Điều này.

Điều 3. Nguyên tắc chung

1. Việc áp dụng Quy định này nhằm phòng ngừa, ngăn chặn các nguy cơ gây mất an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước huyện Nhà Bè.

2. Xác định rõ quyền hạn, trách nhiệm của các cơ quan và cán bộ, công chức, viên chức, người lao động đối với công tác đảm bảo an toàn, an ninh thông tin.

Điều 4. Giải thích từ ngữ

Các từ ngữ trong Quy chế này được hiểu như sau:

1. An toàn thông tin mạng: là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, 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. An ninh mạng: là việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

3. Ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước: là việc sử dụng công nghệ thông tin vào các hoạt động của cơ quan nhà nước nhằm nâng cao chất lượng, hiệu quả trong hoạt động nội bộ của cơ quan nhà nước và giữa các cơ quan nhà nước, trong giao dịch của cơ quan nhà nước với tổ chức và cá nhân; hỗ trợ đẩy mạnh cải cách hành chính và bảo đảm công khai, minh bạch.

4. Phần mềm độc hại: là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay 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. Hệ thống thông tin: là tập hợp 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 trên mạng.

6. Tài khoản người dùng (User Account): mỗi người được cấp một tên riêng không trùng lắp (User name) và mật khẩu (password) để có quyền truy cập hệ thống và sử dụng.

7. Cán bộ phụ trách công nghệ thông tin: là cán bộ, công chức, viên chức, người lao động được tuyển dụng phụ trách an toàn thông tin, công nghệ thông tin tại các cơ quan, đơn vị.

Chương II

QUY ĐỊNH ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 5. Về quản lý cán bộ, công chức, viên chức và người lao động

1. Cán bộ, công chức, viên chức, người lao động phải cam kết tuân thủ thực hiện các quy định bảo đảm an toàn thông tin của đơn vị mình.

2. Các cơ quan, đơn vị thường xuyên phối hợp với Phòng Nội vụ Huyện lập kế hoạch tổ chức đào tạo cho cán bộ, công chức, viên chức và người lao động để nâng cao kiến thức cơ bản và kỹ năng an toàn mạng, an toàn thông tin; đồng thời phổ biến các quy định về an toàn, an ninh thông tin hàng năm để mọi người hiểu rõ các quyền và trách nhiệm đối với việc đảm bảo an toàn, an ninh thông tin. Thường xuyên kiểm tra việc thực hiện các nội quy, quy chế về an toàn, an ninh thông tin đối với cán bộ, công chức, viên chức, người lao động 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.

4. 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.

Điều 6. Quản lý, đảm bảo an toàn hạ tầng công nghệ thông tin

1. Đối với phòng máy chủ:

a) Các khu vực có yêu cầu cao về an toàn, bảo mật như phòng máy chủ, nơi đặt tường lửa (firewall), thiết bị định tuyến (router), hệ thống các máy chủ, các thiết bị lưu trữ… phải áp dụng biện pháp kiểm soát ra vào thích hợp. Phòng máy chủ là khu vực hạn chế tiếp cận và cần 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. 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.

b) Bảo đảm an toàn môi trường vật lý (nhiệt, độ ẩm, ánh sáng,...) cho phòng máy chủ, các hệ thống hỗ trợ (máy điều hòa nhiệt độ, nguồn cấp điện, hệ thống chống sét lan truyền, dự phòng nguồn điện, cáp quang truyền dẫn) được an toàn và hoạt động ổn định, sẵn sàng.

c) Có biện pháp bảo vệ phòng chống nguy cơ do cháy nổ, ngập lụt, động đất và các sự cố khác do thiên nhiên và con người gây ra.

2. Các cơ quan phải thực hiện các biện pháp bảo vệ cần thiết để phòng tránh mất cắp hoặc phá hoại tại các vị trí lắp đặt các thiết bị xử lý và lưu trữ của hệ thống thông tin.

3. Phải bố trí máy tính riêng đã được kiểm tra an ninh, không kết nối mạng nhằm tránh thất thoát thông tin khi soạn thảo các tài liệu mật.

4. Về việc tổ chức mô hình mạng: cài đặt, cấu hình, tổ chức hệ thống mạng theo hướng dẫn của Sở Thông tin và Truyền thông Thành phố, hạn chế sử dụng mô hình mạng ngang hàng. Các đơn vị trực thuộc không nằm trong cùng một khu vực, cần thiết lập hệ thống mạng riêng để đảm bảo an ninh.

5. Về việc sử dụng hệ thống mạng không dây: không kết nối, sử dụng hệ thống mạng không dây vào mạng nội bộ của Ủy ban nhân dân huyện.

6. Chống mã độc, virus: lựa chọn, triển khai các phần mềm chống virus, mã độc có hiệu quả trên các máy chủ, máy trạm làm việc, thiết bị thông minh có kết nối mạng nội bộ; đồng thời, thường xuyên cập nhật phiên bản mới, bản vá lỗi của các phần mềm chống virus, nhằm kịp thời phát hiện, loại trừ mã độc.

Điều 7. Quản lý vận hành, sử dụng hệ thống thông tin

1. Đối với các cơ quan:

a) Trang bị đầy đủ các kiến thức bảo mật cơ bản cho cán bộ, công chức, viên chức trước khi cho phép truy cập và sử dụng hệ thống thông tin.

b) Bố trí cán bộ phụ trách về an toàn hệ thống thông tin. Cán bộ phụ trách được đảm bảo điều kiện học tập, tiếp cận công nghệ, kiến thức an toàn bảo mật thông tin trước khi tiến hành các hoạt động quản lý.

c) Quan tâm và ưu tiên bố trí kinh phí cần thiết để đảm bảo và tăng cường an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của đơn vị.

2. Đối với cán bộ phụ trách công nghệ thông tin tại các đơn vị:

a) Tham mưu cho lãnh đạo triển khai thực hiện các biện pháp để đảm bảo an toàn, an ninh hệ thống thông tin của đơn vị. Thường xuyên nghiên cứu, cập nhật các kiến thức về an toàn, an ninh thông tin, có biện pháp phòng tránh các nguy cơ tiềm ẩn có thể gây mất thông tin.

b) Thường xuyên cập nhật cấu hình chuẩn cho các thành phần của hệ thống thông tin, thiết lập cấu hình chặt chẽ nhất nhưng vẫn đảm bảo duy trì hoạt động thường xuyên của hệ thống thông tin. Khi thiết lập cấu hình hệ thống thông tin chỉ cung cấp những chức năng thiết yếu nhất; xác định các chức năng, cổng giao tiếp mạng, giao thức, và dịch vụ không cần thiết để cấm hoặc hạn chế sử dụng.

c) Thường xuyên thực hiện việc theo dõi bản ghi nhật ký 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. Các rủi ro đó có thể xảy ra do sự truy cập trái phép, sử dụng trái phép, mất, thay đổi hoặc phá hủy thông tin và hệ thống thông tin.

3. Đối với cán bộ, công chức, viên chức và người lao động:

a) Mỗi cán bộ, công chức, viên chức và người lao động phải có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng; đặt mật khẩu cho máy tính. Sử dụng các thiết bị lưu trữ thông tin (USB, ổ cứng gắn ngoài, thẻ nhớ) đảm bảo an toàn, đúng cách để phòng ngừa virus, phần mềm gián điệp xâm nhập máy tính phá hoại, đánh cắp thông tin.

b) Các máy tính khi không sử dụng trong thời gian dài (quá 4 giờ làm việc) cần tắt máy hoặc ngưng kết nối mạng, để tránh bị các tin tặc lợi dụng, sử dụng chức năng điều khiển từ xa dùng máy tính của mình tấn công vào các hệ thống thông tin khác.

c) Phải thực hiện quét virus trước khi mở các tập tin đính kèm theo thư điện tử, không mở các thư điện tử khi chưa rõ người gửi hoặc tập tin đính kèm có nguồn gốc không rõ ràng để tránh virus, phần mềm gián điệp lây nhiễm máy tính.

Điều 8. Bảo vệ bí mật nhà nước trong hoạt động ứng dụng công nghệ thông tin

1. Quy định về soạn thảo, in ấn, phát hành và sao chụp tài liệu mật

a) Không được sử dụng máy tính nối mạng Internet để soạn thảo văn bản; chuyển giao, lưu trữ thông tin có nội dung thuộc bí mật nhà nước; cung cấp tin, tài liệu và đưa thông tin bí mật nhà nước lên Cổng/Trang thông tin điện tử, mạng xã hội.

b) Không được in, sao chụp tài liệu bí mật nhà nước trên các thiết bị kết nối mạng internet.

c) Phải bố trí 01 máy vi tính riêng, không kết nối mạng nội bộ và mạng Internet dùng để quản lý, soạn thảo các tài liệu mật của nhà nước theo quy định.

2. Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật, các đơn vị phải báo cáo cho người có thẩm quyền. Không được cho phép các tổ chức, cá nhân không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố.

3. Trước khi thanh lý các máy tính trong các cơ quan nhà nước, cán bộ phụ trách công nghệ thông tin phải dùng các biện pháp kỹ thuật xoá bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

Điều 9. Quản lý truy cập

1. Quy định về quản lý truy cập vào hệ thống thông tin, mạng máy tính 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 cấp cho một người quản lý và sử dụng.

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

5. Mật khẩu đăng nhập vào các hệ thống thông tin phải có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số và ký tự đặc biệt như: !, @, #, $, %...) và phải được thay đổi ít nhất 3 tháng/lần.

Điều 10. Ứng cứu sự cố an toàn thông tin

1. Phân nhóm sự cố an toàn thông tin:

a) Sự cố do bị tấn công mạng: tấn công từ chối dịch vụ; tấn công giả mạo; tấn công sử dụng mã độc; truy cập trái phép, chiếm quyền điều khiển; tấn công thay đổi giao diện; tấn công mã hóa phần mềm, dữ liệu, thiết bị; phá hoại thông tin, dữ liệu, phần mềm; nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu; các hình thức tấn công mạng khác.

b) Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật.

c) Sự cố do lỗi của người quản trị, vận hành hệ thống.

d) Sự cố liên quan đến tự nhiên như bão, lụt, động đất, hỏa hoạn.

2. Phân loại mức độ 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 đơn vị.

b) Trung bình: sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của đơn vị.

c) Cao: sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và gây ảnh hưởng đến hoạt động chung của cơ quan.

d) Khẩn cấp: sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của cơ quan.

3. Khi có sự cố hoặc nguy cơ mất an toàn thông tin xảy ra, đơn vị phải chỉ đạo kịp thời để khắc phục và hạn chế thiệt hại.

4. Trường hợp có sự cố ở mức độ cao, khẩn cấp vượt quá khả năng khắc phục của đơn vị, đơn vị phải báo cáo ngay cho cơ quan quản lý trực tiếp hoặc Văn phòng Hội đồng nhân dân và Ủy ban nhân dân huyện (Thông qua Tổ Tin học).

Điều 11. Bảo đảm an toàn dữ liệu

1. Thực hiện quy trình sao lưu dự phòng và phục hồi dữ liệu cho các phần mềm, dữ liệu lưu trữ cần thiết khi gặp sự cố.

2. Lập danh sách các dữ liệu, phần mềm cần được sao lưu, có phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian phục hồi hệ thống từ dữ liệu sao lưu.

3. Dữ liệu sao lưu phải được lưu trữ an toàn và được kiểm tra thường xuyên đảm bảo sẵn sàng cho việc sử dụng khi cần.

Điều 12. Các hành vi bị nghiêm cấm

1. Tạo, cài đặt, phát tán thư rác, tin nhắn rác, phần mềm độc hại.

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

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

4. Ngăn chặn việc truy cập 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. Làm mất an toàn, lộ, lọt và phát tán bí mật thông tin của đơn vị, cá nhân; truyền đưa, lưu trữ văn bản, tài liệu mật của đơn vị qua các dịch vụ chia sẻ thông tin trên môi trường mạng.

7. 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 cơ quan quản lý.

Chương III

TRÁCH NHIỆM ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN VÀ TỔ CHỨC THỰC HIỆN

Điều 13. Trách nhiệm của Phòng Văn hóa và Thông tin

1. Chủ trì, phối hợp với Trung tâm Văn hóa - Thể thao và Truyền thông huyện thực hiện tuyên truyền công tác bảo vệ an toàn, an ninh thông tin trong hoạt động công nghệ thông tin trên địa bàn huyện.

2. Phối hợp với Phòng Nội vụ, Phòng Tư pháp huyện tổ chức các hội nghị tuyên truyền, phổ biến pháp luật về an toàn thông tin, an ninh mạng, bảo vệ bí mật nhà nước trên địa bàn huyện.

3. Phối hợp với Văn phòng Hội đồng nhân dân và Ủy ban nhân dân Huyên, Sở Thông tin và Truyền thông thực hiện việc tiếp nhận và xử lý các sự cố về an toàn an ninh mạng tại các đơn vị.

4. Tổng hợp dự toán và đề xuất kinh phí cho công tác đảm bảo an toàn thông tin tại Huyện. Chủ trì, hướng dẫn các cơ quan thực hiện việc đề xuất cấp độ an toàn thông tin theo quy định

5. Phân công một bộ phận hoặc cán bộ phụ trách công nghệ thông tin hỗ trợ kỹ thuật cho các đơn vị, tạo điều kiện để các cán bộ phụ trách công nghệ thông tin được học tập, nâng cao trình độ về an toàn thông tin.

6. Tổng hợp báo cáo về tình hình an toàn, an ninh thông tin theo định kỳ trình Ủy ban nhân dân huyện báo cáo Sở Thông tin và Truyền thông thành phố.

7. Thường xuyên cập nhật những chính sách, thủ tục an toàn thông tin của đơn vị và thực hiện đúng hướng dẫn về an toàn, an ninh thông tin của Sở Thông tin và Truyền thông Thành phố.

Điều 14. Trách nhiệm của Văn phòng Hội đồng nhân dân và Ủy ban nhân dân Huyện.

1. Phối hợp với Sở Thông tin và Truyền thông, Phòng Văn hóa và Thông tin cùng các cơ quan có liên quan trong công tác đảm bảo an toàn, bảo mật đối với hệ thống máy chủ, duy trì kết nối mạng giữa Ủy ban nhân dân huyện với các đơn vị; triển khai các phần mềm chống virus, mã độc hiệu quả trên máy chủ; áp dụng các biện pháp để khắc phục và hạn chế thiệt hại khi sự cố xảy ra.

2.Tham mưu Ủy ban nhân dân huyện vận hành hệ thống thông tin phục vụ chỉ đạo điều hành của Lãnh đạo Ủy ban nhân dân Huyện do Văn phòng Hội đồng nhân dân và Ủy ban nhân dân Huyện quản lý theo quy định tại Quy chế này và phối hợp Phòng Văn hóa và Thông tin thực hiện việc tiếp nhận và xử lý các sự cố về an toàn an ninh mạng tại các đơn vị.

Điều 15. Trách nhiệm của Phòng Nội vụ

1. Chủ trì phối hợp với các đơn vị tổ chức các lớp tập huấn, bồi dưỡng kiến thức về công nghệ thông tin, an toàn thông tin, an ninh mạng trên địa bàn Huyện và các khóa học do Thành phố tổ chức.

2. Phối hợp với Tổ công tác về kiểm tra, xử lý các vi phạm được nêu trong quy chế này.

3. Cập nhật tình hình tổ chức, hoạt động của các đơn vị nhằm có đánh giá làm cơ sở bình xét thi đua hàng năm của các đơn vị.

Điều 16. Trách nhiệm của phòng Tài chính - Kế hoạch

Phối hợp với Phòng Văn hóa và Thông tin và các cơ quan, đơn vị có liên quan, tham mưu Ủy ban nhân dân Huyện bố trí kinh phí thực hiện công tác 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 huyện Nhà Bè.

Điều 17. Trách nhiệm của các cơ quan, đơn vị

1. Thủ trưởng các cơ quan, đơn vị có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trong công tác bảo đảm an toàn thông tin mạng của đơn vị mình;

2. Chỉ đạo công chức, viên chức và người lao động nghiêm túc chấp hành các quy định về bảo đảm an toàn thông tin; thường xuyên tổ chức quán triệt các quy định về an toàn thông tin trong đơn vị. Tạo điều kiện để các cán bộ học tập, nâng cao trình độ về an toàn, an ninh thông tin.

3. Thực hiện bảo đảm an toàn thông tin gồm các nội dung cơ bản như quy định về quản lý hạ tầng mạng, bảo đảm an toàn dữ liệu, bảo đảm an toàn thiết bị và người dùng đầu cuối phù hợp với Quy chế này và các quy định của pháp luật.

4. 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 hiệu quả.

5. Phối hợp chặt chẽ với Công an huyện và các cơ quan, đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin trên không gian mạng.

6. Dự toán và sử dụng kinh phí được bố trí hàng năm cho công tác bảo đảm an toàn thông tin của đơn vị mình; mua phần mềm chống virus có bản quyền... nhằm thực hiện tốt công tác bảo mật, bảo đảm an toàn thông tin mạng.

Điều 18. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các cơ quan, đơn vị

1. Trách nhiệm của cán bộ, công chức, viên chức và người lao động được giao phụ trách công nghệ 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 chế, 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 thông tin.

2. Trách nhiệm của cán bộ, công chức, viên chức, người lao động:

a) Nghiêm túc chấp hành các quy chế của Ủy ban nhân dân huyện và các quy định khác của pháp luật về an toàn, an ninh thông tin. Chịu trách nhiệm đảm bảo an toàn, an ninh thông tin trong phạm vi trách nhiệm và quyền hạn được giao.

b) Mỗi cán bộ, công chức, viên chức và người lao động phải có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản mà mình được giao sử dụng; không cung cấp thông tin tài khoản các ứng dụng của cá nhân, đơn vị cho người khác; không tự ý thay đổi, tháo lắp các thiết bị trên máy tính; không được vào các trang web 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.

c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin để kịp thời ngăn chặn và xử lý.

d) Khuyến khích tham gia các chương trình đào tạo, hội nghị về an toàn, an ninh thông tin, an ninh mạng do Sở Thông tin và Truyền thông tổ chức.

Điều 19. Trách nhiệm của các tổ chức, cá nhân liên quan

Các tổ chức, cá nhân khác có sử dụng các hệ thống thông tin do Ủy ban nhân dân huyện triển khai và liên quan đến hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn huyện phải tuân thủ Quy chế này và các quy định hiện hành của pháp luật.

Điều 20. Tổ chức thực hiện

1. Thủ trưởng các cơ quan, đơn vị, Chủ tịch Ủy ban nhân dân các xã, thị trấn chịu trách nhiệm tổ chức triển khai thực hiện Quy chế tại đơn vị mình.

2. Trong quá trình thực hiện, nếu có những vấn đề cần sửa đổi, bổ sung, hoặc chưa được quy định rõ, các đơn vị gửi kiến nghị, đề xuất về Phòng Văn hóa và Thông tin Huyện để tổng hợp, báo cáo trình Ủy ban nhân dân huyện sửa đổi, bổ sung cho phù hợp với tình hình thực tiễn.

ỦY BAN NHÂN DÂN HUYỆN NHÀ BÈ