ỦY BAN NHÂN DÂN THÀNH PHỐ HẢI PHÒNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 2993/2016/QĐ-UBND	*Hải Phòng, ngày 30 tháng 11 năm 2016*

QUYẾT ĐỊNH

Ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn thành phố Hải Phòng

ỦY BAN NHÂN DÂN THÀNH PHỐ HẢI PHÒNG

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

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

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

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

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

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;

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 67/TTr-STTTT ngày 31/10/2016; Báo cáo thẩm định số 61/BCTĐ-STP ngày 18/10/2016 của Sở Tư pháp,

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 của các cơ quan nhà nước trên địa bàn thành phố Hải Phòng.

Điều 2. Quyết định này có hiệu lực kể từ ngày 15 tháng 12 năm 2016.

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

Nơi nhận:
- Văn phòng Chính phủ;
- Bộ Thông tin & Truyền thông;
- Cục KTVB (Bộ Tư pháp);
- TTTU, TT HĐND TP;
- CT, các PCT UBND TP;
- Đoàn Đại biểu QH thành phố;
- Như Điều 3;
- Sở Tư pháp;
- Đài PTTH HP, Báo HP, Báo ANHP;
- Cổng TTĐT TP, Công báo TP;
- Lưu: VT.

TM. UỶ BAN NHÂN DÂN THÀNH PHỐ
CHỦ TỊCH

Nguyễn Văn Tùng

ỦY BAN NHÂN DÂN THÀNH PHỐ HẢI PHÒNG	CỘNG HÒA 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 của các cơ quan nhà nước trên địa bàn thành phố Hải Phòng

(Ban hành kèm theo Quyết định số 2993/2016/QĐ-UBND ngày 30 / 11 /2016 của UBND thành phố Hải Phòng)

Chương I

QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về hoạt động bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn thành phố Hải Phòng, bao gồm: Quản lý bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin; trách nhiệm bảo đảm an toàn, an ninh thông tin đối với các hệ thống thông tin và kiểm tra công tác bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin.

Điều 2. Đối tượng áp dụng

1. Quy chế này được áp dụng đối với các cơ quan nhà nước trên địa bàn thành phố Hải Phòng, bao gồm: Các cơ quan chuyên môn thuộc Ủy ban nhân dân thành phố, Ủy ban nhân dân các quận, huyện, Ủy ban nhân dân các xã, phường, thị trấn trên địa bàn thành phố; đơn vị sự nghiệp công lập trực thuộc Ủy ban nhân dân thành phố; đơn vị sự nghiệp công lập trực thuộc cơ quan chuyên môn thuộc Ủy ban nhân dân thành phố và đơn vị sự nghiệp công lập trực thuộc Ủy ban nhân dân quận, huyện trên địa bàn thành phố (sau đây gọi tắt là cơ quan, đơn vị).

2. Cán bộ, công chức, viên chức, người lao động đang làm việc trong các cơ quan, đơn vị nêu tại Khoản 1 Điều này áp dụng Quy chế này trong việc vận hành, khai thác hệ thống thông tin tại các cơ quan, đơn vị và tổ chức, cá nhân khác có liên quan.

Điều 3. Nguyên tắc đảm bảo an toàn, an ninh thông tin

Các hoạt động ứng dụng công nghệ thông tin phải tuân theo nguyên tắc bảo đảm 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 và Điều 4 Luật An toàn thông tin mạng.

Điều 4. Giải thích từ ngữ

1. Các thuật ngữ: "An toàn thông tin mạng", "Mạng", "Hệ thống thông tin", "Đơn vị chuyên trách về công nghệ thông tin" được hiểu theo quy định của Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015; Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ.

2. Tường lửa là rào chắn (phần cứng, phần mềm) được lập ra nhằm kiểm soát người dùng mạng Internet truy nhập vào các thông tin không mong muốn và người dùng từ bên ngoài truy nhập trái phép thông tin trong mạng nội bộ.

3. TCVN 7562:2005: Tiêu chuẩn Việt Nam về mã thực hành quản lý an toàn thông tin.

4. TCVN ISO/IEC 27001:2009: Tiêu chuẩn Việt Nam về Hệ thống quản lý an toàn thông tin.

5. TCVN 7816:2007: Tiêu chuẩn Việt Nam về Kỹ thuật mật mã thuật toán mã dữ liệu theo chuẩn mã hóa nâng cao.

6. Ban Chỉ đạo 114: Ban Chỉ đạo lực lượng phản ứng nhanh về ứng phó, xử lý sự cố an ninh, an toàn thông tin mạng được Ủy ban nhân dân thành phố Hải Phòng thành lập tại Quyết định số 787/QĐ-UBND ngày 17/4/2015.

Chương II

QUY ĐỊNH ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 5. Điều kiện đảm bảo thực hiện nhiệm vụ an toàn, an ninh thông tin

1. Các cơ quan, đơn vị phải phổ biến những kiến thức cơ bản về an toàn, an ninh thông tin cho cán bộ, công chức, viên chức, người lao động trước khi tham gia sử dụng hệ thống thông tin.

2. Các cơ quan, đơn vị bố trí cán bộ làm công tác chuyên trách về công nghệ thông tin phải có chuyên ngành phù hợp và được đào tạo, bồi dưỡng chuyên môn đối với lĩnh vực an toàn, an ninh thông tin.

3. Xác định và ưu tiên phân bổ kinh phí cần thiết cho các hoạt động liên quan đến việc bảo vệ hệ thống thông tin, thông qua việc đầu tư các thiết bị tường lửa, các chương trình chống thư rác, vi-rút máy tính trên hệ thống máy chủ, máy trạm và các công tác khác liên quan đến việc bảo đảm an toàn, an ninh thông tin.

4. Cán bộ tham gia đoàn kiểm tra công tác đảm bảo an toàn, an ninh thông tin phải được trang bị đầy đủ những kiến thức và được tập huấn hàng năm về công tác đảm bảo an toàn, an ninh thông tin.

5. Các cơ quan, đơn vị phải xây dựng, ban hành quy chế nội bộ về đảm bảo an toàn, an ninh thông tin; phải căn cứ các nội dung của tiêu chuẩn TCVN 7562:2005 và TCVN ISO 27001:2009 để quy định rõ các vấn đề sau:

a) Mục tiêu, phạm vi và đối tượng áp dụng.

b) Quy định cụ thể quyền và trách nhiệm của từng đối tượng: Lãnh đạo đơn vị, Lãnh đạo cấp phòng, cán bộ chuyên trách về công nghệ thông tin và người sử dụng.

c) Quy định về cấp phát, thu hồi, cập nhật và quản lý các tài khoản truy cập vào hệ thống thông tin phải đảm bảo chặt chẽ, đúng quy định của pháp luật.

d) Quy định về an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của đơn vị.

đ) Cơ chế sao lưu dữ liệu, cơ chế báo cáo và phối hợp khắc phục sự cố.

e) Theo dõi, kiểm tra, thống kê, tổng hợp, báo cáo theo định kỳ và đột xuất.

h) Tổ chức thực hiện.

6. Thực hiện xác định cấp độ an toàn hệ thống thông tin theo quy định tại Điều 14 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.

Điều 6. Trang thiết bị và hạ tầng công nghệ thông tin

1. Phòng máy chủ:

a) Các thiết bị mạng quan trọng như tường lửa, thiết bị định tuyến, hệ thống máy chủ và các trang thiết bị mạng phải được đặt trong phòng máy chủ và có các biện pháp bảo vệ, ngăn chặn xâm nhập trái phép vào phòng máy chủ; phải có hệ thống lưu điện đủ công suất và duy trì được thời gian hoạt động của các máy chủ tối thiểu 30 phút khi xảy ra sự cố mất điện. Trong trường hợp do yêu cầu bắt buộc thì phải lắp đặt máy phát điện để đảm bảo hệ thống thiết bị và máy chủ được duy trì liên tục.

b) Chỉ những người có trách nhiệm theo quy định của Thủ trưởng cơ quan mới được phép vào phòng máy chủ; quá trình vào, ra phòng máy chủ phải được ghi nhận vào nhật ký quản lý phòng máy chủ.

c) Bố trí cán bộ có năng lực chuyên môn cao để quản lý, vận hành phòng máy chủ và duy trì chế độ trực phù hợp để bảo đảm an toàn thông tin mạng.

2. Máy chủ: Cấu hình máy chủ phải đủ mạnh để đáp ứng công việc. Máy chủ của các cơ quan, đơn vị chỉ dùng để triển khai phần mềm hệ thống, các dữ liệu lưu trữ cần thiết và các phần mềm chống vi-rút.

3. Thiết bị chống sét, phòng cháy, chữa cháy: Các cơ quan, đơn vị phải lắp đặt thiết bị chống sét, trang bị thiết bị phòng cháy, chữa cháy cho phòng máy chủ theo quy định pháp luật.

4. Thiết bị chuyển mạch: Thiết bị chuyển mạch mạng tin học của các cơ quan phải đảm bảo khả năng cung cấp các chức năng quản trị nhằm tăng cường độ an toàn và bảo mật cho hệ thống mạng như: Cung cấp khả năng từ chối các kết nối không mong muốn hay trái phép vào hệ thống và khống chế số lượng kết nối vào hệ thống mạng nội bộ thông qua thiết bị chuyển mạch. Phải có ít nhất 01 thiết bị chuyển mạch hỗ trợ định tuyến cho mỗi mạng nội bộ, hỗ trợ chức năng điều khiển truy cập, chức năng xác thực thiết bị, xác thực người sử dụng và chức năng bảo mật quản trị mạng.

5. Tường lửa: Các cơ quan, đơn vị phải xây dựng tường lửa đảm bảo các yêu cầu gồm khả năng xử lý được số lượng kết nối đồng thời cao và chịu được thông lượng cao, hỗ trợ các công nghệ mạng riêng ảo thông dụng và có khả năng mã hoá dữ liệu, cung cấp đầy đủ các cơ chế bảo mật cơ bản, quản lý luồng dữ liệu ra, vào và có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ.

Điều 7. Quy định về quản trị phần mềm ứng dụng

Trong quá trình đầu tư, thiết kế, xây dựng, nâng cấp các phần mềm hệ thống, các phần mềm ứng dụng dùng chung trong các cơ quan nhà nước phải đáp ứng yêu cầu quản trị, vận hành đảm bảo an toàn, an ninh thông tin mạng.

1. Quản lý tài nguyên: Cán bộ quản trị mạng có trách nhiệm kiểm tra, giám sát chức năng chia sẻ thông tin; tổ chức cấp phát tài nguyên trên máy chủ theo danh mục thư mục cho từng phòng/ban; khuyến cáo người dùng cân nhắc việc chia sẻ tài nguyên cục bộ trên máy đang sử dụng, tuyệt đối không được chia sẻ toàn bộ ổ cứng. Khi thực hiện chia sẻ tài nguyên trên máy chủ hoặc trên máy cục bộ phải sử dụng mật khẩu để bảo vệ thông tin.

2. Quản lý đăng nhập hệ thống: Các hệ thống thông tin cần giới hạn số lần đăng nhập vào hệ thống. Hệ thống tự động khoá tài khoản hoặc cô lập tài khoản khi liên tục đăng nhập sai vượt quá số lần quy định. Tổ chức theo dõi, giám sát tất cả các phương tiện đăng nhập từ xa.

3. Quản lý tài khoản, định danh người dùng trong các hệ thống thông tin, bao gồm: tạo mới, kích hoạt, sửa đổi và loại bỏ các tài khoản, đồng thời tổ chức kiểm tra các tài khoản của hệ thống thông tin ít nhất 6 tháng/lần thông qua các công cụ của hệ thống. Hủy tài khoản, quyền truy cập và thu hồi các thiết bị liên quan tới hệ thống (thiết bị lưu trữ khóa, thẻ nhận dạng) đối với cán bộ, công chức, viên chức đã chuyển công tác hoặc nghỉ việc.

4. Quản lý nhật ký: Hệ thống thông tin phải ghi nhận các sự kiện như: Quá trình đăng nhập vào hệ thống, các thao tác cấu hình hệ thống. Thường

xuyên kiểm tra, sao lưu các nhật ký truy nhập theo từng tháng để lưu vết theo dõi, xác định những sự kiện đã xảy ra của hệ thống và hạn chế việc tràn bản ghi nhật ký gây ảnh hưởng đến hoạt động của hệ thống.

5. Quản lý cài đặt: Các phần mềm được cài đặt trên máy chủ phục vụ công tác chuyên môn nghiệp vụ, điều hành phải có kế hoạch được lãnh đạo cơ quan, đơn vị phê duyệt. Cán bộ, công chức, viên chức không được tự ý cài đặt thêm phần mềm khác trên máy tính cá nhân nhằm tránh sự lây lan của vi-rút. Cán bộ chuyên trách công nghệ thông tin có trách nhiệm kiểm tra, cài đặt và chịu trách nhiệm về mức độ an toàn, bảo mật các phần mềm ứng dụng phục vụ công tác chuyên ngành tại các máy tính công vụ của cán bộ, công chức, viên chức. Các phần mềm cài đặt trên máy chủ phải có bản quyền, không cài đặt các phần mềm không rõ nguồn gốc vào máy chủ để phòng lây nhiễm mã độc.

6. Xung đột phần mềm: Trong quá trình thiết kế, nâng cấp các phần mềm chuyên ngành phải đảm bảo tương thích và tích hợp được với các phần mềm dùng chung đảm bảo tránh được các xung đột và gây mất an toàn thông tin.

Điều 8. Phòng chống mã độc, vi-rút, tấn công mạng

1. Tất cả các máy trạm, máy chủ, các thiết bị công nghệ thông tin trong mạng và hệ thống thông tin phải được cài đặt phần mềm chống mã độc, vi-rút phù hợp. Các phần mềm phòng chống mã độc, vi-rút phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc, vi-rút 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 mã độc, các rủi ro do mã độc 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 các tập tin trên các thiết bị lưu trữ di động.

4. Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng.

5. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm mã độc, vi-rút trên máy chủ, máy trạm, thiết bị công nghệ thông tin (như: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu, những dấu hiệu sai khác bất thường) người sử dụng phải tắt máy và báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý.

Điều 9. Bảo vệ thông tin trong hoạt động ứng dụng công nghệ thông tin

1. Mỗi cơ quan, đơn vị đã nêu tại Điều 2 của Quy chế này phải trang bị ít nhất 01 máy tính, 01 máy in, 01 máy hủy tài liệu, không kết nối với các thiết bị có khả năng phát tán thông tin ra bên ngoài, không kết nối với các thiết bị lưu

trữ dữ liệu bên ngoài nhằm phục vụ cho công tác soạn thảo, lưu trữ và hủy văn bản có nội dung thuộc danh mục bí mật nhà nước.

2. Không được phép chụp hình, ghi âm, ghi hình những cuộc họp, hội nghị, hội thảo, tập huấn có quy định không được sử dụng các thiết bị điện tử.

3. Các thiết bị công nghệ thông tin, phần mềm lưu trữ dữ liệu thuộc danh mục bí mật nhà nước được mua sắm mới phải đảm bảo hàng chính hãng, xuất xứ rõ ràng, có bản quyền phần mềm, có bảo hành từ 12 tháng trở lên. Khi nhận bàn giao thiết bị mua mới hoặc thiết bị sau sửa chữa, phải kiểm tra đầy đủ các thông số kỹ thuật, rà quét đề phòng sự xâm nhập của các phần mềm gián điệp hoặc có gắn mã độc.

4. Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật, các thiết bị, phần mềm lưu trữ thông tin có độ mật, phải báo cáo cho cơ quan có thẩm quyền. Không được cho phép các tổ chức, đơn vị hoặc người không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố.

5. Trước khi thanh lý hoặc điều chuyển các máy tính, thiết bị lưu trữ không còn nhu cầu sử dụng trong các cơ quan nhà nước, phải dùng các biện pháp kỹ thuật kiểm tra, sao lưu, xoá bỏ vĩnh viễn dữ liệu trong thiết bị lưu trữ, ổ cứng máy tính, tránh lộ lọt thông tin.

Điều 10. Quản lý, vận hành hệ thống thông tin của đơn vị

1. Hệ thống thông tin của các cơ quan, đơn vị phải có cơ chế sao lưu dữ liệu ở mức hệ thống, dữ liệu của các ứng dụng, dữ liệu của người sử dụng; cơ chế sao lưu dữ liệu phải được thực hiện thường xuyên; thiết bị lưu trữ dữ liệu được sao lưu phải đảm bảo yêu cầu kỹ thuật; dữ liệu được sao lưu phải đảm bảo tính sẵn sàng và toàn vẹn đáp ứng yêu cầu phục hồi dữ liệu cho hệ thống thông tin hoạt động bình thường khi có sự cố xảy ra.

2. Hệ thống thông tin của các cơ quan, đơn vị phải được triển khai cơ chế bảo mật, an toàn thông tin bằng các thiết bị phần cứng và phần mềm phù hợp với quy mô của đơn vị.

3. Hệ thống thông tin của đơn vị phải được triển khai chức năng giám sát truy cập từ ngoài vào hệ thống, từ hệ thống gửi ra bên ngoài; ghi lại nhật ký ra/vào hệ thống để phục vụ công tác khắc phục sự cố, điều tra, phân tích và làm rõ các nguy cơ gây ra mất an toàn, an ninh thông tin; chức năng không cho người dùng truy cập một số trang thông tin điện tử không phù hợp với quy định hiện hành.

4. Hệ thống mạng không dây của các cơ quan, đơn vị phải được thiết lập khoá khi truy cập tối thiểu theo tiêu chuẩn Việt Nam TCVN 7816:2007.

5. Mạng riêng ảo của các cơ quan, đơn vị kết nối để truy cập vào hệ thống thông tin phải được bảo mật; quản lý và kiểm soát chặt chẽ các kết nối; hủy bỏ kết nối khi không còn sử dụng.

6. Tất cả các tài khoản truy cập vào hệ thống máy chủ, thiết bị mạng, máy tính, các ứng dụng phải được thiết lập mật khẩu; mật khẩu phải được đặt ở mức bảo mật cao (số lượng ký tự và nội dung của mật khẩu); mật khẩu có tối thiểu 6 ký tự bao gồm chữ hoa, chữ thường, chữ số và ký tự đặc biệt; phải thường xuyên thay đổi mật khẩu với tần suất phù hợp; danh sách tài khoản phải được quản lý, kiểm tra và cập nhật kịp thời; quyền truy cập của tài khoản phải được thiết lập phù hợp cho từng đối tượng.

7. Việc di chuyển thiết bị công nghệ thông tin từ nơi này đến nơi khác phải có sự đồng ý của lãnh đạo và giám sát chặt chẽ việc đảm bảo an toàn an ninh thông tin. Tránh hỏng hóc mất mát thiết bị và các dữ liệu.

8. Việc tạo lập, xử lý và hủy bỏ dữ liệu cần được kiểm tra, giám sát chặt chẽ, đảm bảo tính toàn vẹn, dữ liệu quan trọng không bị thất thoát ra ngoài hoặc tạo lập không đầy đủ.

Điều 11. Cán bộ chuyên trách về công nghệ thông tin

1. Được đảm bảo điều kiện về đào tạo, bồi dưỡng, học tập, nghiên cứu, tiếp thu kiến thức, kỹ thuật và công nghệ mới đối với lĩnh vực an toàn, an ninh thông tin.

2. Quản lý chặt chẽ việc di chuyển các trang thiết bị công nghệ thông tin lưu trữ các thông tin thuộc danh mục bí mật nhà nước.

3. Thực hiện cấp phát, thu hồi, cập nhật và quản lý tất cả các tài khoản truy cập vào hệ thống thông tin của đơn vị; hướng dẫn người sử dụng thay đổi mật khẩu ngay sau khi đăng nhập lần đầu tiên; bảo vệ thông tin của tài khoản theo quy định.

4. Triển khai áp dụng các giải pháp tổng thể đảm bảo an toàn, an ninh thông tin mạng trong toàn hệ thống; triển khai các giải pháp kỹ thuật phòng chống vi-rút, mã độc hại, thư rác cho hệ thống và máy tính cá nhân; kiểm soát và có giải pháp kỹ thuật chống truy cập trái phép vào hệ thống thông tin.

5. Thường xuyên cập nhật các bản vá lỗi đối với hệ thống, cập nhật các phiên bản mới đối với chương trình chống vi-rút.

6. Thường xuyên sao lưu dữ liệu theo quy định; kiểm tra dữ liệu sao lưu phải đảm bảo tính sẵn sàng, tin cậy và toàn vẹn.

7. Thường xuyên thực hiện phân tích, đánh giá và báo cáo các rủi ro và nguy cơ gây mất an toàn, an ninh thông tin đối với hệ thống thông tin của đơn

vị; nguyên nhân gây ra các rủi ro và nguy cơ gây mất an toàn, an ninh thông tin mạng bao gồm: Hiện tượng tự nhiên (nhiệt độ, không khí, mưa bão, sét), truy cập trái phép, vi-rút, cố ý làm thay đổi thông số cấu hình hệ thống và phá hủy dữ liệu. Đồng thời tham mưu và xây dựng phương án hạn chế, khắc phục các rủi ro và nguy cơ có thể xảy ra.

8. Kiểm soát chặt chẽ cài đặt phần mềm vào máy trạm và máy chủ.

Điều 12. 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;

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;

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;

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

2. Khi có sự cố hoặc nguy cơ mất an toàn thông tin thì lãnh đơn vị phải chỉ đạo kịp thời để khắc phục và hạn chế thiệt hại, báo cáo 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 13. Các hành vi bị nghiêm cấm

Các hành vi bị nghiêm cấm tuân theo quy định tại Điều 12 và Khoản 2 Điều 72 Luật Công nghệ thông tin, Điều 8 Luật An toàn thông tin mạng và các quy định pháp luật hiện hành khác có liên quan.

Chương III

TRÁCH NHIỆM ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN MẠNG

Điều 14. Trách nhiệm của Sở Thông tin và Truyền thông

1. Tham mưu giúp Ủy ban nhân dân thành phố thực hiện quản lý nhà nước về an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn thành phố.

2. Thực hiện công tác tham mưu Ủy ban nhân dân thành phố ban hành:

a) Văn bản chỉ đạo, đề án, kế hoạch nhằm đảm bảo an toàn, an ninh thông tin.

b) Xây dựng tiêu chuẩn đánh giá mức độ an toàn, an ninh thông tin đối với hệ thống thông tin của các cơ quan, đơn vị trên địa bàn thành phố.

c) Xây dựng danh mục các loại phần mềm được phép triển khai cài đặt tại Trung tâm dữ liệu điện tử để đảm bảo sử dụng hiệu quả hạ tầng dùng chung và cơ sở dữ liệu tập trung; Danh mục các phần mềm chuyên ngành, phần mềm thương mại được phép cài đặt trên máy tính của cán bộ, công chức, viên chức để đảm bảo an toàn, an ninh thông tin và tiết kiệm ngân sách nhà nước.

d) Xây dựng danh mục các phần mềm bắt buộc vận hành trong hệ thống mạng truyền số liệu chuyên dùng của thành phố và danh mục những phần mềm có thể triển khai trên hệ thống mạng Internet.

đ) Thành lập Đoàn kiểm tra liên ngành về đảm bảo an toàn, an ninh thông tin mạng trong hoạt động ứng dụng công nghệ thông tin trong các cơ quan nhà nước do Sở Thông tin và Truyền thông chủ trì phối hợp với các cơ quan liên quan.

3. Hàng năm, tổ chức đào tạo chuyên sâu về an toàn, an ninh thông tin mạng cho lực lượng đảm bảo an toàn, an ninh thông tin mạng của các cơ quan, đơn vị.

4. Thực hiện nhiệm vụ cảnh báo về nguy cơ hoặc sự cố mất an toàn, an ninh thông tin.

5. Tổ chức Hội nghị, Hội thảo chuyên đề về an toàn, an ninh thông tin.

6. Phối hợp với Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam và các đơn vị có liên quan trong thực hiện nhiệm vụ đảm bảo an toàn, an ninh thông tin mạng.

7. Phối hợp với Công an thành phố, Ban chỉ đạo 114 và các cơ quan, đơn vị có liên quan tổ chức đoàn kiểm tra về an toàn, an ninh thông tin mạng để kịp thời phát hiện, xử lý các hành vi vi phạm theo quy định của pháp luật; kiểm tra trang thiết bị và hạ tầng công nghệ thông tin của các cơ quan, đơn vị.

8. Chủ động hướng dẫn các cơ quan, đơn vị xây dựng quy chế nội bộ, hỗ trợ kỹ thuật, nội dung, thời gian báo cáo công tác đảm bảo an toàn, an ninh thông tin.

9. Tổng hợp báo cáo và thông báo về tình hình an toàn, an ninh thông tin mạng 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.

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

11. Giải quyết các vấn đề liên quan kỹ thuật đảm bảo khả năng tích hợp các phần mềm dùng chung vào hệ thống thông tin của thành phố.

12. Chỉ đạo Trung tâm Thông tin và Truyền thông đảm bảo kỹ thuật, tổ chức thực hiện các biện pháp bảo đảm an toàn, an ninh thông tin trên mạng máy tính của các cơ quan nhà nước trên địa bàn thành phố; hỗ trợ kỹ thuật cho các đơn vị trong việc ngăn chặn, phòng ngừa và khắc phục sự cố liên quan đến an toàn, an ninh thông tin trên mạng máy tính.

13. Hằng năm, Sở Thông tin và Truyền thông dựa trên kết quả kiểm tra, đánh giá, báo cáo công tác an toàn, an ninh thông tin của các cơ quan, đơn vị, đề xuất xác lập bảng xếp hạng an toàn, an ninh thông tin; trên cơ sở đó, báo cáo đề xuất Chủ tịch Ủy ban nhân dân thành phố xem xét khen thưởng cho các cá nhân, đơn vị có thành tích đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin theo quy định hiện hành.

Điều 15. Trách nhiệm của Công an thành phố, Ban chỉ đạo 114

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 chịu trách nhiệm quản lý, kiểm soát, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống thông tin gây phương hại đến an toàn, an ninh thông tin mạng trong cơ quan nhà nước.

2. Chủ trì, phối hợp với Sở Thông tin và Truyền thông và các cơ quan, đơn vị có liên quan tổ chức Đoàn kiểm tra về an toàn, an ninh thông tin mạng để kịp thời phát hiện, xử lý các hành vi vi phạm theo quy định của pháp luật; kiểm tra trang thiết bị và hạ tầng công nghệ thông tin của các cơ quan, đơn vị. Trường hợp đặc biệt phức tạp, cần phối hợp với Cục nghiệp vụ Bộ Công an để đảm bảo an ninh, an toàn thông tin cho hạ tầng công nghệ thông tin của các cơ quan, đơn vị thành phố.

3. Tăng cường công tác tuyên truyền, phổ biến pháp luật; tổ chức phòng ngừa, phát hiện, đấu tranh và xử lý nghiêm các hoạt động xâm hại đến an toàn, an ninh thông tin.

4. Điều tra và xử lý các trường hợp vi phạm pháp luật về lĩnh vực an toàn, an ninh thông tin mạng 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.

Điều 16. Trách nhiệm của Sở Nội vụ, Sở Tài chính

Sở Nội vụ tổng hợp kế hoạch đào tạo, bồi dưỡng kiến thức, nghiệp vụ an toàn thông tin cho cán bộ, công chức, viên chức trong hoạt động ứng dụng công

nghệ thông tin hàng năm của Sở Thông tin và Truyền thông và các cơ quan, đơn vị có liên quan trình Ủy ban nhân dân thành phố ban hành.

Sở Tài chính chủ trì, phối hợp với Sở Thông tin và Truyền thông, Công an thành phố, Ban chỉ đạo 114 và các cơ quan, đơn vị có liên quan trong việc bố trí kinh phí thực hiện nhiệm vụ bảo đảm an toàn, an ninh thông tin theo quy định.

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

1. Trách nhiệm của thủ trưởng các cơ quan, đơn vị:

a) Thủ trưởng cơ quan chuyên môn thuộc Ủy ban nhân dân thành phố chịu trách nhiệm trước Ủy ban nhân dân thành phố trong công tác đảm bảo an toàn, an ninh thông tin đối với toàn bộ hệ thống thông tin của đơn vị mình và các đơn vị sự nghiệp công lập trực thuộc (nếu có);

b) Chủ tịch Ủy ban nhân dân cấp huyện trên địa bàn thành phố chịu trách nhiệm trước Ủy ban nhân dân thành phố trong công tác đảm bảo an toàn, an ninh thông tin đối với toàn bộ hệ thống thông tin của đơn vị mình và các Ủy ban nhân dân cấp xã thuộc phạm vi quản lý, đơn vị sự nghiệp công lập trực thuộc (nếu có);

c) Chủ tịch Ủy ban nhân dân cấp xã chịu trách nhiệm trước Ủy ban nhân dân cấp huyện trong công tác đảm bảo an toàn, an ninh thông tin đối với toàn bộ hệ thống thông tin của đơn vị mình;

d) Thủ trưởng đơn vị sự nghiệp công lập chịu trách nhiệm trước cơ quan chủ quản trong công tác đảm bảo an toàn, an ninh thông tin đối với toàn bộ hệ thống thông tin của đơn vị mình.

2. Thực hiện và chỉ đạo cán bộ, công chức, viên chức, người lao động thuộc thẩm quyền quản lý thực hiện nghiêm túc Quy chế này.

3. Tạo điều kiện thuận lợi cho cán bộ chuyên trách về công nghệ thông tin được đào tạo, bồi dưỡng chuyên môn trong lĩnh vực an toàn, an ninh thông tin mạng.

4. Quan tâm đầu tư các thiết bị phần cứng, phần mềm liên quan đến công tác đảm bảo an toàn, an ninh thông tin; xây dựng và ban hành quy chế đảm bảo an toàn cho hệ thống thông tin của đơn vị mình quản lý.

5. Bố trí kinh phí và các nguồn lực cho đào tạo, tập huấn, mua sắm, sửa chữa, thay thế về cơ sở vật chất, trang thiết bị công nghệ thông tin và phần mềm diệt vi-rút có bản quyền tại đơn vị.

6. Khi có sự cố hoặc nguy cơ mất an toàn, an ninh thông tin mạng phải chỉ đạo khắc phục sự cố kịp thời, hạn chế thấp nhất mức thiệt hại có thể xảy ra, ưu tiên sử dụng lực lượng kỹ thuật tại chỗ của đơn vị mình, đồng thời lập biên bản và báo cáo bằng văn bản cho cơ quan có liên quan; 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.

7. Tổ chức kiểm tra an ninh, an toàn các thiết bị, phần mềm hệ thống, phần mềm ứng dụng trước khi đưa vào sử dụng tại các bộ phận quan trọng, cơ mật, nơi chứa đựng bí mật nhà nước, bí mật nội bộ thuộc cơ quan, đơn vị. Các thiết bị, phần mềm do tổ chức cá nhân, nước ngoài tài trợ phải được kiểm định an toàn trước khi sử dụng.

8. Khi xây dựng các dự án, công trình công nghệ thông tin, các cơ quan, đơn vị phải gửi thiết kế kỹ thuật xin ý kiến tham vấn của Sở Thông tin và Truyền thông về công tác đảm bảo an toàn, an ninh thông tin.

9. Phối hợp với Công an thành phố, Sở Thông tin và Truyền thông và các cơ quan chức năng tăng cường công tác đảm bảo an toàn, an ninh thông tin; thường xuyên tuyên truyền, phổ biến cho cán bộ, công chức, viên chức, người lao động hiểu rõ tầm quan trọng về đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của đơn vị.

Điều 18. Trách nhiệm của cán bộ, công chức, viên chức tại các cơ quan, đơn vị

1. Trách nhiệm của cán bộ chuyên trách công nghệ thông tin:

a) Chịu trách nhiệm triển khai các biện pháp quản lý vận hành, quản lý kỹ thuật và tham mưu xây dựng các quy định về đảm bảo an toàn, an ninh thông tin mạng cho hoạt động ứng dụng công nghệ thông tin của đơn vị mình đúng theo nội dung Quy chế này.

b) Chủ động phối hợp với cá nhân, đơn vị có liên quan trong việc kiểm tra, phát hiện và khắc phục sự cố về an toàn, an ninh thông tin; tuân thủ theo sự hướng dẫn kỹ thuật của Sở Thông tin và Truyền thông trong quá trình khắc phục sự cố về an toàn, an ninh thông tin.

c) Thường xuyên cập nhật, nâng cao kiến thức, trình độ chuyên môn đáp ứng yêu cầu đảm bảo an toàn thông tin của đơn vị.

2. Trách nhiệm của cán bộ, công chức, viên chức tham gia sử dụng và khai thác hệ thống thông tin:

a) Nghiêm túc thực hiện các nội quy, quy chế, quy trình nội bộ về đảm bảo an toàn, an ninh thông tin mạng của đơn vị cũng như các quy định khác của pháp luật về nội dung này.

b) Khi phát hiện nguy cơ hoặc sự cố mất an toàn, an ninh thông tin phải báo cáo kịp thời cho cán bộ chuyên trách công nghệ thông tin của đơn vị mình để kịp thời ngăn chặn và xử lý.

c) Nâng cao ý thức cảnh giác và trách nhiệm về an toàn, an ninh thông tin.

d) Tham gia các chương trình đào tạo, hội nghị về an toàn, an ninh thông tin do cơ quan có thẩm quyền tổ chức.

Điều 19. Trách nhiệm của các doanh nghiệp cung cấp hạ tầng mạng và dịch vụ Internet.

Các doanh nghiệp cung cấp hạ tầng mạng viễn thông và dịch vụ internet phải thiết lập đầu mối liên lạc để phối hợp và tuân thủ việc điều phối của cơ quan chức năng và tham gia vào công tác ứng cứu, khắc phục sự cố cho hệ thống thông tin quan trọng của thành phố.

Chương IV
KIỂM TRA CÔNG TÁC ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN MẠNG

Điều 20. Trách nhiệm và phối hợp trong công tác kiểm tra

1. Sở Thông tin và Truyền thông phối hợp với Công an thành phố, Ban Chỉ đạo 114 và các đơn vị có liên quan tham mưu cho Ủy ban nhân dân thành phố tổ chức kiểm tra công tác đảm bảo an toàn, an ninh thông tin định kỳ hàng năm đối với các cơ quan, đơn vị trên địa bàn thành phố.

2. Công an thành phố cử cán bộ phối hợp, tham gia đoàn kiểm tra, đánh giá công tác đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan, đơn vị; điều tra và xử lý các trường hợp vi phạm các quy định về an toàn, an ninh thông tin mạng theo thẩm quyền.

3. Các cơ quan, đơn vị liên quan được mời tham gia đoàn kiểm tra: Cử cán bộ có chuyên môn về công nghệ thông tin tham gia đoàn kiểm tra; phối hợp với đoàn kiểm tra xây dựng các tiêu chí và quy trình kỹ thuật kiểm tra công tác đảm bảo an toàn, an ninh thông tin.

4. Công an thành phố, Ban Chỉ đạo 114 tiến hành kiểm tra đột xuất các cơ quan, đơn vị khi phát hiện có dấu hiệu vi phạm pháp luật về an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin theo đúng quy định của pháp luật.

5. Đối với việc kiểm tra định kỳ, Đoàn kiểm tra có trách nhiệm thông báo thời gian, địa điểm, nội dung và thành phần cho đơn vị được kiểm tra biết trước ít nhất 05 ngày để chuẩn bị.

6. Đơn vị được kiểm tra:

a) Chuẩn bị nội dung báo cáo theo yêu cầu của Đoàn kiểm tra.

b) Có đại diện lãnh đạo và cán bộ chuyên trách công nghệ thông tin của đơn vị để cùng làm việc với Đoàn kiểm tra.

c) Tạo thuận lợi cho công tác kiểm tra đạt kết quả.

Điều 21. Kiểm tra định kỳ và đột xuất

1. Đoàn kiểm tra xây dựng kế hoạch và thực hiện kiểm tra định kỳ hàng năm 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.

2. Đoàn kiểm tra tiến hành kiểm tra đột xuất các cơ quan, đơn vị có dấu hiệu vi phạm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin.

Điều 22. Điều khoản thi hành

1. Sở Thông tin và Truyền thông chủ trì, phối hợp với các cơ quan, đơn vị có liên quan triển khai thực hiện tốt nội dung Quy chế này.

2. Các cơ quan, đơn vị chủ động xây dựng, ban hành Quy chế nội bộ về đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin tại đơn vị mình phù hợp với Quy chế này. Định kỳ hàng năm báo cáo tổng hợp tình hình đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin tại đơn vị gửi Sở Thông tin và Truyền thông trước ngày 15 tháng 11 để tổng hợp, báo cáo Ủy ban nhân dân thành phố./.

TM. ỦY BAN NHÂN DÂN THÀNH PHỐ
CHỦ TỊCH

Nguyễn Văn Tùng