UỶ BAN NHÂN DÂN **THÀNH PHỐ HÀ NỘI**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 411 /QĐ-UBND	*Hà Nội, ngày 27 tháng 01 năm 2015*

QUYẾT ĐỊNH

Về việc ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước Thành phố Hà Nội

ỦY BAN NHÂN DÂN THÀNH PHỐ HÀ NỘI

Căn cứ Luật Tổ chức Hội đồng nhân dân và Uỷ ban nhân dân ngày 26/11/2003;

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

Căn cứ Pháp lệnh Số 30/2000/PL-UBTVQH10 ngày 28/12/2000 của Ủy Ban Thường Vụ Quốc Hội về việc Bảo vệ bí mật Nhà nước;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 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 07 năm 2013 của Chính phủ hướng dẫn về Quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng;

Căn cứ Thông tư số 27/2011/TT-BTTTT ngày 4/10/2011 của Bộ Thông tin và Truyền thông Quy chế về điều phối các hoạt động ứng cứu sự cố mạng Internet Việt Nam;

Xét đề nghị của Giám đốc Sở Thông tin và Truyền thông Thành phố Hà Nội tại Tờ trình số 2247/TTr-STTTT ngày 25/12/ 2014,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo quyết định này Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước thành phố Hà Nội.

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

Điều 3. Chánh Văn phòng UBND Thành phố, Giám đốc các sở, Chủ tịch UBND các quận, huyện thị xã, Thủ trưởng các ban, ngành, các tổ chức và cá nhân có liên quan chịu trách nhiệm thi hành quyết định này./.

Nơi nhận:
- Như Điều 3;
- TTTU; TTHĐND TP; (để b/c)
- Đ/c Chủ tịch UBND TP; (để b/c)
- Các đ/c Phó Chủ tịch UBND TP;
- Cổng giao tiếp Điện tử HN;
- VPUBTP: Đ/c CVP, các đ/c PVP, THCB, TH;
- Lưu: VT, VX Dg.

4409. (150.)

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Nguyễn Thị Bích Ngọc

ỦY BAN NHÂN DÂN THÀNH PHỐ HÀ NỘI	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY CHẾ

Đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước Thành phố Hà Nội

(Ban hành kèm theo Quyết định số 411 /QĐ-UBND ngày 27 tháng 01 năm 2015 của Ủy ban nhân dân thành phố Hà Nội)

Điều 1. Phạm vi điều chỉnh

Quy chế này điều chỉnh về công tác đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin (gọi tắt là CNTT) của các cơ quan nhà nước Thành phố Hà Nội.

Điều 2. Đối tượng áp dụng

1. Quy chế này áp dụng đối với các cơ quan nhà nước thành phố Hà Nội, bao gồm: Các sở, ban, ngành, các đơn vị trực thuộc UBND thành phố; UBND các quận, huyện, thị xã, UBND các phường, xã, thị trấn và các đơn vị trực thuộc (sau đây gọi tắt là đơn vị).

2. Cán bộ, công chức, viên chức và người lao động đang làm việc tại các đơn vị quy định tại khoản 1 điều này.

Điều 3. Nguyên tắc chung

1. Việc bảo đảm an toàn thông tin là yêu cầu bắt buộc trong quá trình thiết kế, xây dựng, vận hành, nâng cấp, sử dụng và huỷ bỏ trong ứng dụng CNTT của cơ quan nhà nước.

2. Thủ trưởng đơn vị là người chịu trách nhiệm trực tiếp chỉ đạo công tác đảm bảo an toàn thông tin.

3. Xác định rõ quyền hạn, trách nhiệm của thủ trưởng, các phòng, ban và từng cá nhân trong đơn vị đối với công tác đảm bảo an toàn thông tin.

4. Các đơn vị xây dựng, triển khai quy chế đảm bảo an toàn thông tin, đảm bảo tuân thủ theo các nội dung tại quy chế này.

5. Bố trí nguồn lực phù hợp với quy mô, điều kiện của đơn vị nhằm thực hiện tốt nhất công tác đảm bảo an toàn thông tin.

Điều 4. Giải thích từ ngữ

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

1. An toàn thông tin: bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và

nội dung thông tin đối với nguy cơ tự nhiên hoặc do con người gây ra. Việc bảo vệ thông tin, tài sản và con người trong hệ thống thông tin nhằm bảo đảm cho các hệ thống thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy. An toàn thông tin bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng.

2. Cán bộ được giao phụ trách đảm bảo an toàn thông tin: là cán bộ kỹ thuật hoặc cán bộ quản lý được giao phụ trách công tác bảo đảm an toàn, an ninh thông tin cho việc triển khai, vận hành, khai thác hệ thống CNTT tại đơn vị.

3. Bên thứ ba: là các tổ chức, cá nhân có chuyên môn được đơn vị thuê hoặc hợp tác với đơn vị nhằm cung cấp hàng hóa, dịch vụ kỹ thuật cho hệ thống CNTT.

4. Tài sản CNTT: là các trang thiết bị, thông tin thuộc hệ thống công nghệ thông tin của đơn vị bao gồm:

a) Tài sản vật lý: là các thiết bị công nghệ thông tin, phương tiện truyền thông và các thiết bị phục vụ hoạt động của hệ thống công nghệ thông tin (bao gồm cả các tài sản hỗ trợ như thiết bị điều hòa, UPS,...);

b) Tài sản thông tin: là các dữ liệu, tài liệu liên quan đến hệ thống công nghệ thông tin.

c) Tài sản phần mềm: là các chương trình ứng dụng, phần mềm hệ thống, cơ sở dữ liệu và công cụ phát triển.

Điều 5. Quản lý tài sản CNTT

1. Đơn vị phải thống kê, kiểm kê tài sản CNTT (tài sản vật lý, tài sản thông tin, tài sản phần mềm) tối thiểu mỗi năm 1 lần.

2. Đơn vị có trách nhiệm kiểm tra, đánh giá mức độ an toàn đối với các tài sản CNTT trước khi đưa vào sử dụng. Trước khi đưa vào sử dụng, đơn vị có thể đề nghị cơ quan công an kiểm tra, đánh giá đối với các thiết bị CNTT sử dụng tại các cơ quan trọng yếu, phục vụ các công việc yêu cầu đảm bảo bí mật,...

3. Việc quản lý, sử dụng các tài sản CNTT khi thực hiện các hoạt động có liên quan đến nước ngoài (đi công tác nước ngoài, giao dịch, làm việc với các tổ chức nước ngoài,..) thực hiện theo quy định của thành phố và nhà nước. Các thiết bị CNTT sử dụng khi đi công tác nước ngoài phải được kiểm tra trước và sau mỗi chuyến công tác.

4. Thông tin liên quan đến tài sản (loại tài sản, số hiệu, vị trí, thông tin bản quyền, các mô tả khác cho việc thay thế, phục hồi, khắc phục sửa lỗi nhanh) cần được lưu trữ, quản lý và cập nhật kịp thời.

5. Phân loại tài sản công nghệ thông tin (vật lý, thông tin, dữ liệu) theo mức độ giá trị, độ nhạy cảm, tầm ảnh hưởng đối với hệ thống, tần suất sử dụng, thời

gian lưu trữ để xây dựng nội quy, biện pháp kỹ thuật nghiệp vụ phù hợp (định kỳ sao lưu dữ liệu, bảo trì hệ thống…).

6. Gắn quyền sử dụng tài sản cho các cá nhân hoặc bộ phận cụ thể. Người sử dụng tài sản CNTT phải tuân thủ các quy định về quản lý, sử dụng tài sản, đảm bảo tài sản được sử dụng đúng mục đích và an toàn.

7. Phải xây dựng kế hoạch kiểm tra, bảo dưỡng tài sản theo định kỳ. Trang thiết bị lưu trữ thông tin khi không sử dụng nữa cần phải được hủy bỏ, việc hủy bỏ đảm bảo tránh mất mát dữ liệu và không thể phục hồi.

8. Việc kiểm tra, đánh giá về khả năng đảm bảo an toàn thông tin đối với các tài sản CNTT thực hiện theo các quy định của pháp luật và hướng dẫn của cơ quan chức năng.

9. Khi bên thứ ba thực hiện việc cung cấp, bảo dưỡng, sửa chữa tài sản CNTT cho đơn vị, phải thực hiện việc quản lý đảm bảo an toàn thông tin của đơn vị như sau:

a) Đánh giá về năng lực kỹ thuật, nhân sự, khả năng tài chính của bên thứ ba trước khi ký kết hợp đồng cung cấp hàng hóa, dịch vụ;

b) Xác định rõ trách nhiệm, quyền hạn và nghĩa vụ của các bên về đảm bảo an toàn thông tin khi ký hợp đồng. Hợp đồng với bên thứ ba phải bao gồm các điều khoản về việc xử lý khi có vi phạm quy chế an toàn, bảo mật thông tin và trách nhiệm phải bồi thường thiệt hại của bên thứ ba trong trường hợp có thiệt hại do hành vi vi phạm của bên thứ ba gây ra;

c) Chú ý đến các vấn đề về tính bí mật, tính toàn vẹn, tính sẵn sàng, tin cậy, hiệu năng tối đa, khả năng phục hồi thảm họa, phương tiện lưu trữ của hệ thống thông tin khi có sự tham gia của bên thứ ba;

d) Áp dụng các biện pháp giám sát chặt chẽ và giới hạn quyền truy cập của bên thứ ba khi cho phép truy cập vào hệ thống CNTT của đơn vị.

Điều 6. Quản lý nguồn nhân lực

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

2. Các cá nhân trong đơn vị liên quan đến bảo mật thông tin phải ký cam kết bảo mật thông tin.

3. Cần phải bố trí nhân sự có năng lực, chất lượng và đạo đức đảm nhận vị trí chuyên trách cho công tác bảo đảm an toàn thông tin, quản trị hệ thống công nghệ thông tin của đơn vị.

4. Đơn vị phải lập kế hoạch 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, cập nhật các quy chế về an toàn thông tin hàng năm

để mọi người hiểu rõ các quyền và trách nhiệm đối với việc đảm bảo an toàn thông tin.

5. Trước khi phân công nhiệm vụ, đơn vị cần xác định yêu cầu về đảm bảo an toàn thông tin của vị trí phân công. Kiểm tra lý lịch, xem xét đánh giá tư cách đạo đức, trình độ chuyên môn khi phân công, giao nhiệm vụ cho cán bộ, công chức, viên chức và người lao động làm việc tại các vị trí trọng yếu của hệ thống CNTT như quản trị hệ thống, quản trị hệ thống an ninh bảo mật, vận hành hệ thống, quản trị cơ sở dữ liệu.

6. Trong thời gian làm việc, đơn vị có trách nhiệm: Phổ biến và cập nhật các quy chế về an toàn thông tin; thường xuyên kiểm tra việc thực hiện các nội quy, quy chế về an toàn thông tin của đơn vị đối với cán bộ, công chức, viên chức, người lao động theo định kỳ.

7. Khi chấm dứt hoặc thay đổi công việc, đơn vị phải: Xác định rõ trách nhiệm của cán bộ, công chức, viên chức và người lao động và các bên liên quan về hệ thống CNTT; thu hồi hoặc thay đổi quyền truy cập hệ thống CNTT cho phù hợp với công việc được thay đổi.

8. Đối với bên thứ 3, trong quá trình triển khai đơn vị cần:

a) Yêu cầu bên thứ ba cung cấp danh sách nhân sự tham gia và yêu cầu bên thứ ba ký cam kết không tiết lộ thông tin của đơn vị đối với các thông tin quan trọng;

b) Cung cấp và yêu cầu bên thứ ba tuân thủ đầy đủ các quy chế về an toàn thông tin của đơn vị và giám sát quá trình thực hiện;

c) Trong trường hợp phát hiện dấu hiệu vi phạm hoặc vi phạm quy chế an toàn, bảo mật thông tin của bên thứ ba, đơn vị cần: Tạm dừng hoặc đình chỉ hoạt động của bên thứ ba tùy theo mức độ vi phạm; thông báo chính thức các vi phạm về an toàn, bảo mật CNTT của nhân sự cho bên thứ ba; kiểm tra xác định, lập báo cáo mức độ vi phạm và thông báo cho bên thứ ba thiệt hại xảy ra; thu hồi ngay quyền truy cập hệ thống CNTT đã được cấp cho bên thứ ba;

d) Sau khi kết thúc công việc: Yêu cầu bên thứ ba bàn giao lại tài sản sử dụng của đơn vị trong quá trình triển khai công việc; thu hồi quyền truy cập hệ thống CNTT đã được cấp của bên thứ ba ngay sau khi kết thúc công việc; thay đổi các khóa, mật khẩu nhận bàn giao từ bên thứ ba.

Điều 7. Quản lý, đảm bảo an toàn hạ tầng ứng dụng CNTT

1. Đối với khu vực đặt trang thiết bị CNTT:

a) Các khu vực có yêu cầu cao về an toàn, bảo mật như phòng máy chủ phải áp dụng biện pháp kiểm soát ra vào thích hợp, đảm bảo chỉ những người có nhiệm vụ mới được vào khu vực đó;

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, 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 thảm họa khác do thiên nhiên và con người gây ra. Có nội quy, hướng dẫn làm việc trong khu vực an toàn, bảo mật.

2. Đơn vị phải thực hiện các biện pháp bảo vệ cần thiết để phòng tránh mất cắp hoặc phá hoại tại các khu lắp đặt các thiết bị xử lý và lưu trữ của hệ thống thông tin, chỉ những người có quyền, nhiệm vụ mới được phép vào. Đặc biệt là khu vực xử lý, lưu trữ thông tin quan trọng, nhạy cảm của đơn vị cần phải trang bị cơ chế kiểm tra xác thực nâng cao (thẻ, token, vân tay...).

3. Chủ động thực hiện việc phân tích và đánh giá các mối đe dọa khách quan như bão lũ, cháy nổ, lở đất, vật liệu độc hại, hoặc các mối đe dọa khác do thiên nhiên và có kế hoạch phòng chống.

4. 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.

5. Hệ thống máy chủ phải được dán nhãn, có sơ đồ đấu nối, thể hiện cụ thể về địa chỉ IP, tên máy chủ. Sơ đồ đấu nối phải được cập nhật nếu có sự thay đổi.

6. Ứng dụng chữ ký số chuyên dùng để đảm bảo an toàn, an ninh thông tin trong việc triển khai ứng dụng CNTT trong hoạt động cơ quan nhà nước và phục vụ công dân, tổ chức.

7. Về việc tổ chức mô hình mạng: Cài đặt, cấu hình, tổ chức hệ thống mạng theo mô hình mạng phân lớp, hạn chế sử dụng mô hình mạng ngang hàng. Các đơn vị có nhiều phòng, ban, đơn vị trực thuộc không nằm trong cùng một khu vực, cần thiết lập hệ thống mạng riêng bảo mật để đảm bảo an ninh cho mạng nội bộ.

8. Về việc quản lý hệ thống mạng không dây: Khi thiết lập mạng không dây cho phép các thiết bị kết nối với mạng cục bộ qua hình thức không dây tại các điểm truy nhập, điểm đấu nối của thiết bị không dây vào mạng nội bộ cần ở lớp ngoài của mạng (khu vực không bảo mật), thiết bị không dây cần được thiết lập các tham số như: tên, mật khẩu, mã hóa dữ liệu… và thông báo các thông tin liên quan đến điểm truy nhập để cơ quan sử dụng, thường xuyên thay đổi mật khẩu nhằm tăng cường công tác bảo mật.

9. Chống mã độc, virus: Lựa chọn, triển khai các phần mềm chống virus, mã độc có hiệu quả trên các máy chủ, máy trạm, các thiết bị, phương tiện kỹ thuật trong mạng, các hệ thống thông tin quan trọng như: Cổng/Trang thông tin điện tử,

thư điện tử, một cửa điện tử,...; 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 máy tính.

Điều 8. Đảm bảo an toàn trong quá trình vận hành, khai thác sử dụng các hệ thống thông tin

1. Tùy theo tình hình thực tế triển khai ứng dụng CNTT, các đơn vị cần thực hiện việc quản lý và kiểm soát mạng nhằm ngăn ngừa các hiểm họa và duy trì an toàn cho các hệ thống, ứng dụng sử dụng mạng. Các nội dung có thể bao gồm:

a) Sử dụng thiết bị tường lửa, thiết bị phát hiện và ngăn chặn xâm nhập trái phép và các trang thiết bị khác đảm bảo an toàn bảo mật mạng;

b) Thiết lập, cấu hình đầy đủ các tính năng của thiết bị an ninh mạng;

c) Sử dụng các công cụ để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng và các truy cập bất hợp pháp vào hệ thống mạng;

d) Thường xuyên kiểm tra, phát hiện những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào mạng.

2. Quản lý bản ghi nhật ký hệ thống: Hệ thống thông tin cần ghi nhận đầy đủ thông tin trong các bản ghi nhật ký khi thao tác trên hệ thống và lưu giữ nội dung nhật ký trong khoảng thời gian nhất định, để phục vụ việc quản lý, kiểm soát hệ thống thông tin. 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 có thể xảy ra do sự truy cập trái phép, sử dụng trái phép, xóa mất, thay đổi hoặc phá hủy thông tin và hệ thống thông tin.

3. Quản lý đăng nhập hệ thống: Các hệ thống thông tin cần giới hạn một số hữu hạn lần đăng nhập sai liên tiếp. Tổ chức theo dõi, và kiểm soát tất cả các phương pháp truy nhập từ xa tới hệ thống thông tin; yêu cầu người dùng đặt mật khẩu với độ an toàn cao.

4. Tổ chức quản lý tài nguyên: 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 sử dụng cân nhắc việc chia sẻ tài nguyên cục bộ trên máy đang sử dụng, khi thực hiện việc chia sẻ tài nguyên cần phải sử dụng mật khẩu để bảo vệ thông tin.

5. Khai thác, sử dụng các ứng dụng, hệ thống thông tin theo đúng chức năng, nhiệm vụ được giao, đảm bảo phục vụ tốt công tác chuyên môn, nghiệp vụ của đơn vị, phục vụ công dân, doanh nghiệp.

6. Trong quá trình vận hành hệ thống cần thực hiện quy định về phòng chống vi rút, mã độc đáp ứng các yêu cầu cơ bản như: Định kỳ kiểm tra, diệt vi

rút, mã độc và phương tiện mang thông tin, dữ liệu nhận từ bên ngoài trước khi sử dụng; không mở các thư điện tử lạ, các tệp tin đính kèm hoặc các liên kết trong các thư lạ để tránh vi rút, mã độc; không vào các trang web không có nguồn gốc xuất xứ rõ ràng, đáng ngờ; báo ngay cho người quản trị hệ thống xử lý trong trường hợp phát hiện nhưng không diệt được vi rút, mã độc; Không tự ý cài đặt các phần mềm khi chưa được phép của người quản trị hệ thống.

7. Đối với bên thứ ba:

a) Thực hiện giám sát và kiểm tra các dịch vụ do bên thứ ba cung cấp đảm bảo mức độ cung cấp dịch vụ, khả năng hoạt động hệ thống đáp ứng đúng theo thỏa thuận đã ký kết;

b) Đảm bảo triển khai, duy trì các biện pháp an toàn, bảo mật của dịch vụ do bên thứ ba cung cấp theo đúng thỏa thuận;

c) Quản lý các thay đổi đối với các dịch vụ của bên thứ ba cung cấp bao gồm: Nâng cấp phiên bản mới; sử dụng các kỹ thuật mới, các công cụ và môi trường phát triển mới;

d) Đánh giá đầy đủ tác động của việc thay đổi, đảm bảo an toàn khi được đưa vào sử dụng.

Điều 9. Quản lý và khắc phục sự cố, lưu trữ và dự phòng

1. Các sự kiện sự cố an toàn thông tin dưới đây cần được xem xét phân loại và xử lý theo quy chế tại khoản 2,3 điều này, bao gồm:

a) Những truy cập trái phép, hành vi vi phạm tính bảo mật và tính toàn vẹn dữ liệu, ứng dụng;

b) Phát hiện mã độc, tấn công từ chối dịch vụ;

c) Phát hiện ra điểm yếu, lỗ hổng bảo mật của hạ tầng, hệ điều hành, ứng dụng;

d) Hệ thống trục trặc nhiều lần hoặc quá tải;

e) Mất thiết bị, phương tiện công nghệ thông tin;

f) Không tuân thủ chính sách an toàn thông tin hoặc các chỉ dẫn bắt buộc của đơn vị hoặc hành vi vi phạm an ninh vật lý;

g) Các trục trặc của phần mềm hay phần cứng không khắc phục được gây ảnh hưởng đến hoạt động của hệ thống CNTT;

h) Các sự cố khác gây gián đoạn, ảnh hưởng đến hoạt động bình thường của các ứng dụng CNTT tại đơn vị.

2. Đơn vị cần 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 đoán 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 thì lãnh đạo đơn vị phải chỉ đạo kịp thời:

a) Áp dụng mọi biện pháp để khắc phục và hạn chế thiệt hại do sự cố xảy ra, lập biên bản báo cáo cho cơ quan cấp trên quản lý trực tiếp;

b) 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 (mẫu báo cáo về sự cố mất an toàn thông tin quy định tại Phụ lục 1 kèm theo Quyết định này);

c) Tạo điều kiện thuận lợi cho cơ quan chức năng tham gia khắc phục sự cố và thực hiện theo đúng hướng dẫn;

d) Cung cấp đầy đủ, chính xác, kịp thời những thông tin cần thiết cho cơ quan cấp trên quản lý trực tiếp;

e) Báo cáo bằng văn bản về sự cố cho cơ quan cấp trên quản lý trực tiếp và cơ quan quản lý nhà nước.

4. Tất cả công chức, viên chức, người lao động và bên thứ 3 khi phát hiện các sự cố của đơn vị cần thực hiện việc báo cáo với đơn vị đó nhằm ngăn chặn các sự cố an toàn thông tin.

5. Thiết lập cơ chế sao lưu và phục hồi hệ thống:

a) Ban hành và thực hiện quy trình sao lưu dự phòng và phục hồi cho các phần mềm, dữ liệu cần thiết;

b) 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 kiểm tra phục hồi hệ thống từ dữ liệu sao lưu;

c) 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;

d) Kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu tối thiểu sáu tháng một lần.

Điều 10. Đảm bảo an toàn thông tin các ứng dụng, cơ sở hạ tầng dùng chung và trong tích hợp ứng dụng và chia sẻ dữ liệu.

1. Trong quá trình khai thác, vận hành và sử dụng các ứng dụng, cơ sở hạ tầng dùng chung, các đơn vị tham gia phải tuân thủ các quy chế về đảm bảo an toàn thông tin theo yêu cầu của từng hệ thống, ứng dụng, đặc biệt là các ứng dụng, hạ tầng dùng chung của thành phố, bao gồm:

a) Khai thác mạng tin học diện rộng của Thành phố (WAN);

b) Sử dụng và vận hành Trung tâm dữ liệu nhà nước thành phố;

c) Khai thác sử dụng hệ thống thư điện tử;

d) Cổng thông tin điện tử, các phần mềm dùng chung: Quản lý văn bản và Hồ sơ công việc, hệ thống Một cửa điện tử,...

2. Trong quá trình triển khai việc tích hợp ứng dụng, chia sẻ dữ liệu, cần triển khai các giải pháp đảm bảo an toàn thông tin cho từng ứng dụng và trong quá trình chia sẻ dữ liệu cũng như làm rõ trách nhiệm của từng đơn vị, từng ứng dụng tham gia vào hệ thống.

Điều 11. Ban hành và triển khai qui chế đảm bảo an toàn thông tin tại đơn vị

1. Các đơn vị phải xây dựng quy chế nội bộ bảo đảm an toàn cho hệ thống thông tin, trong đó bao gồm các nội dung sau:

a) Yêu cầu và nguyên tắc của công tác bảo đảm an toàn an ninh;

b) Yêu cầu về quản lý tài sản CNTT của đơn vị;

c) Yêu cầu về quản lý nguồn nhân lực;

d) Yêu cầu về quản lý, đảm bảo an toàn môi trường mạng;

e) Yêu cầu về đảm bảo an toàn vận hành các hệ thống thông tin;

f) Quản lý sự cố, lưu trữ và dự phòng;

g) Phân công trách nhiệm và tổ chức thực hiện.

2. Các đơn vị phải tổ chức giám sát việc thực hiện quy chế bảo đảm an toàn cho hệ thống thông tin sau khi được ban hành.

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 được giao 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 chế, 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;

e) 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 trong các đơn vị:

a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ 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) 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;

c) 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;

d) Tham gia các chương trình đào tạo, hội nghị về an toàn an ninh thông tin được thành phố hoặc đơn vị tổ chức.

Điều 13. Trách nhiệm của các đơn vị

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

2. 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.

3. Xây dựng quy chế, quy trình nội bộ về đảm bảo an toàn thông tin 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 đạt hiệu quả.

5. 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.

6. Định kỳ hàng năm, các cơ quan lập báo cáo về tình hình an toàn thông tin và gửi về Sở Thông tin và Truyền thông trước ngày 15/1 của năm tiếp theo.

Điều 14. 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.

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

3. Xây dựng khung quy chế mẫu về đảm bảo an toàn an ninh thông tin để các đơn vị tham khảo, điều chỉnh và áp dụng phù hợp với tình hình từng đơn vị.

4. Chủ trì, phối hợp với Văn phòng Ủy ban nhân dân Thành phố, Công an Thành phố và các đơn vị có liên quan tiến hành kiểm tra công tác bảo đảm an toàn, an ninh thông tin định kỳ hàng năm đối với các đơn vị quản lý nhà nước thuộc Thành phố.

5. Tùy theo mức độ sự cố, phối hợp Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố thông tin.

6. 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 đơn vị có liên quan.

7. Hàng năm xây dựng và triển khai các chương trình đào tạo về an toàn, an ninh thông tin cho lực lượng đảm bảo an toàn, an ninh thông tin của các đơn vị. 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.

Điều 15. Trách nhiệm của Công an thành phố

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

2. Xử lý các trường hợp vi phạm pháp luật về an toàn, an ninh thông tin theo thẩm quyền.

3. Hỗ trợ các đơn vị thực hiện việc kiểm tra, đánh giá các tài sản CNTT trước khi đưa vào sử dụng khi có yêu cầu.

Điều 16. Tổ chức thực hiện

Trong quá trình thực hiện nếu có các vấn đề nảy sinh, không phù hợp hoặc chưa được quy định rõ, các đơn vị gửi kiến nghị, đề xuất về Sở Thông tin và Truyền thông để tổng hợp báo cáo Ủy ban nhân dân Thành phố kịp thời điều chỉnh, bổ sung cho phù hợp với tình hình thực tiễn./.

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Nguyễn Thị Bích Ngọc