ỦY BAN NHÂN DÂN THÀNH PHỐ ĐÀ NẴNG	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số:4159/QĐ-UBND	*Đà Nẵng, ngày 14 tháng 9 năm 2018*

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn thông tin trong lĩnh vực ứng dụng công nghệ thông tin trên địa bàn thành phố Đà Nẵng

ỦY BAN NHÂN DÂN THÀNH PHỐ ĐÀ NẴNG

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

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

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

Căn cứ Luật Giao dịch điện tử ngày 29 tháng 11 năm 2005;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về việc 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 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống theo cấp độ;

Căn cứ Nghị định số 108/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ quy định chi tiết điều kiện kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng;

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

Căn cứ Quyết định số 632/QĐ-TTg ngày 10 tháng 5 năm 2017 của Thủ tướng Chính phủ ban hành Danh mục lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng và hệ thống thông tin quan trọng quốc gia;

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 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Căn cứ Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;

Xét đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 583/TTr-STTTT ngày 15 tháng 6 năm 2018 và Công văn số 1950/STTTT-CNTT ngày 24 tháng 8 năm 2018,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin trong lĩnh vực ứng dụng công nghệ thông tin trên địa bàn thành phố Đà Nẵng.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký và thay thế Quyết định số 9976/QĐ-UBND ngày 21 tháng 11 năm 2011 của UBND thành phố Đà Nẵng ban hành Quy chế bảo đảm an toàn, an ninh thông tin trong lĩnh vực ứng dụng công nghệ thông tin của các cơ quan quản lý hành chính nhà nước thuộc thành phố Đà Nẵng.

Điều 3. Chánh Văn phòng UBND thành phố Đà Nẵng, Giám đốc các sở, ban, ngành; Chủ tịch UBND các quận, huyện, phường, xã và Thủ trưởng các cơ quan, đơn vị, cá nhân liên quan chịu trách nhiệm thi hành Quyết định này./.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH
Huỳnh Đức Thơ

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

QUY CHẾ
Bảo đảm an toàn thông tin trong lĩnh vực ứng dụng công nghệ thông tin trên địa bàn thành phố Đà Nẵng

(Ban hành kèm theo Quyết định số: 4159/QĐ-UBND ngày 14 tháng 9 năm 2018 của Ủy ban nhân dân thành phố Đà Nẵng)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh

Quy chế này quy định các nội dung, biện pháp và trách nhiệm bảo đảm an toàn thông tin trong lĩnh vực ứng dụng công nghệ thông tin (CNTT) trên địa bàn thành phố Đà Nẵng.

2. Đối tượng áp dụng

a) Quy chế này được áp dụng đối với tất cả các cơ quan là sở, ban, ngành; UBND các quận, huyện, phường, xã và các tổ chức, đơn vị sự nghiệp do UBND thành phố Đà Nẵng quyết định thành lập (sau đây gọi chung là cơ quan);

b) Quy chế áp dụng đối với cán bộ, công chức, viên chức, người lao động (CBCCVC-NLĐ) làm việc tại các cơ quan thuộc UBND thành phố Đà Nẵng;

c) Khuyến nghị các tổ chức, cá nhân khác trên địa bàn thành phố Đà Nẵng áp dụng Quy chế này trong công tác bảo đảm an toàn thông tin.

Điều 2. Giải thích từ ngữ

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

1. An toàn thông tin (ATTT) là sự bảo vệ các hệ thống thông tin nhằm phòng, chống và tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép bảo đảm tính toàn vẹn, tính bảo mật và tính khả dụng của thông tin.

2. Hệ thống thông tin (HTTT) 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.

3. HTTT quan trọng của thành phố Đà Nẵng là HTTT mà khi bị phá hoại sẽ gây tổn hại nghiêm trọng đến hoạt động quản lý, điều hành của chính quyền thành phố và trật tự an toàn xã hội trên địa bàn thành phố Đà Nẵng. Danh mục HTTT quan trọng của thành phố Đà Nẵng chi tiết tại Phụ lục I kèm theo Quy chế này.

4. Chủ quản HTTT là cơ quan, tổ chức có thẩm quyền quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hoặc cơ quan, tổ chức được cấp có thẩm quyền giao quản lý HTTT đó.

5. Đơn vị vận hành HTTT là cơ quan, tổ chức được chủ quản HTTT giao để vận hành HTTT đó. Trong trường hợp chủ quản HTTT thuê ngoài dịch vụ CNTT, đơn vị vận hành HTTT là bên cung cấp dịch vụ.

6. Sự cố ATTT là trường hợp HTTT và Thông tin bị truy nhập, sử dụng, tiết lộ trái phép hoặc Hệ thống có sự can thiệp cố ý của con người gây ra việc gián đoạn làm ảnh hưởng đến tính toàn vẹn, tính bảo mật và tính khả dụng của thông tin.

7. Ứng cứu sự cố ATTT là hoạt động nhằm xử lý, khắc phục sự cố ATTT, bao gồm: theo dõi, thu thập, phân tích, phát hiện, cảnh báo, điều tra, xác minh và khắc phục sự cố bảo đảm khôi phục lại để HTTT hoạt động trở lại bình thường.

8. Đội ứng cứu sự cố ATTT thành phố Đà Nẵng (sau đây gọi tắt Đội ứng cứu sự cố) là bộ phận thuộc Ban Chỉ đạo Ứng dụng và Phát triển công nghệ thông tin thành phố Đà Nẵng, có trách nhiệm tham gia ứng cứu xử lý các sự cố ATTT trên địa bàn thành phố Đà Nẵng và phối hợp để tham gia hoạt động khi có yêu cầu từ Bộ Thông tin và Truyền thông hoặc các cơ quan có liên quan.

9. Rủi ro ATTT là những nhân tố chủ quan hoặc khách quan có thể xảy ra trong quá trình vận hành các HTTT hoặc ứng cứu sự cố ATTT.

10. Đánh giá rủi ro ATTT là việc phát hiện, phân tích, ước lượng mức độ tổn hại, mối đe dọa đối với thông tin, HTTT.

11. Mật khẩu có độ phức tạp cao là mật khẩu có độ dài tối thiểu 12 ký tự, trong đó kết hợp bao gồm ký tự hoa, thường, chữ số và ký tự đặc biệt.

12. Bản ghi nhật ký hệ thống (logfile) là tập tin được tạo ra trên thiết bị hoặc chương trình của HTTT, nhằm ghi lại tất cả các tác vụ xảy ra trên thiết bị hoặc chương trình.

Điều 3. Các hành vi bị nghiêm cấm

1. Ngăn chặn việc truyền tải thông tin trên mạng, can thiệp, truy nhập, tiết lộ, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin, dữ liệu của tổ chức, cá nhân.

2. Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của HTTT, có những tác động chủ ý gây ra sự cố ATTT.

3. Phát tán thư rác, phần mềm độc hại, thiết lập HTTT giả mạo, lừa đảo, chiếm quyền điều khiển... phá hoại HTTT.

4. Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của HTTT để thu thập, khai thác thông tin cá nhân.

Chương II
BIỆN PHÁP BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 4. Bảo đảm an toàn thông tin mức vật lý

Đơn vị quản lý, vận hành các máy chủ và các thiết bị mạng có trách nhiệm thực hiện các biện pháp bảo đảm ATTT mức vật lý như sau:

1. Các thiết bị mạng liên quan đến ATTT như tường lửa, thiết bị định tuyến, chuyển mạch, các máy chủ, hệ thống lưu trữ SAN (Storage Area Network), NAS (Network Attached Storage),... phải được đặt trong phòng máy chủ.

2. Phòng máy chủ phải được bố trí ở khu vực riêng biệt, bảo đảm an toàn nhiệt độ, độ ẩm, có trang bị camera, thiết bị bảo đảm an ninh (thiết lập cơ chế bảo vệ, theo dõi, phát hiện xâm nhập trái phép và các biện pháp kiểm soát truy nhập bằng thẻ từ, vân tay), có đầy đủ thiết bị phòng cháy, chữa cháy, nguồn cung cấp điện ổn định và có nguồn điện dự phòng.

3. Phòng máy chủ phải xây dựng quy trình ra, vào phòng máy chủ và phải được ghi nhận trong nhật ký quản lý, các cơ quan quản lý phòng máy chủ có trách nhiệm xây dựng nội quy, hướng dẫn và mô tả các vị trí công việc tại phòng máy.

Điều 5. Bảo đảm an toàn hạ tầng mạng

Đơn vị quản lý, vận hành hạ tầng mạng có trách nhiệm thực hiện các biện pháp sau:

1. Quản lý hạ tầng mạng nội bộ

a) Tuân thủ các quy định kiến trúc hệ thống, tiêu chuẩn, quy chuẩn kỹ thuật; cài đặt, cấu hình, tổ chức hệ thống mạng phù hợp với các tiêu chuẩn ứng dụng CNTT của các cơ quan nhà nước, bảo đảm ATTT, hạn chế sử dụng mô hình mạng có nguy cơ ATTT cao.

b) Đối với các cơ quan có nhiều phòng, ban, đơn vị trực thuộc có trụ sở làm việc không nằm trong cùng một khu vực, khi cấu hình kết nối trên hệ thống mạng đô thị (MAN) thành phố phải thiết lập mạng riêng ảo (Virtual Private Network - VPN).

c) Trang bị thiết bị tường lửa chuyên dụng hoặc phần mềm tường lửa để ngăn chặn và phát hiện xâm nhập trái phép vào mạng nội bộ của cơ quan khi kết nối với hệ thống bên ngoài.

d) Khi thực hiện truy nhập từ xa vào mạng nội bộ thực hiện chức năng quản trị, phải sử dụng giao thức mạng có mã hóa thông tin như SSL/TLS, VPN,... và thiết lập mật khẩu có độ phức tạp cao.

2. Quản lý mạng không dây

a) Khi thiết lập mạng không dây để kết nối với mạng cục bộ thông qua các điểm truy nhập (Access Point - AP), đơn vị vận hành phải thiết lập các tham số: tên, nhận dạng dịch vụ (Service Set Identifier - SSID), mật khẩu có độ phức tạp cao, cấp phép truy nhập đối với địa chỉ vật lý (MAC Address), mã hóa dữ liệu theo cơ chế bảo mật

WPA2 hoặc WPA3.

b) Mật khẩu đăng nhập phải được thiết lập có độ phức tạp cao, định kỳ 3 tháng thay đổi mật khẩu nhằm tăng cường công tác bảo mật.

c) Khi cung cấp truy cập Internet qua mạng không dây cho người ngoài cơ quan, đơn vị vận hành phải tạo thêm một SSID riêng và giới hạn băng thông truy cập phù hợp đối với đối tượng này.

Điều 6. Bảo đảm an toàn máy chủ

1. Trên hệ thống máy chủ các đơn vị chủ quản, vận hành phải:

a) Hệ điều hành được cài đặt là phần mềm có bản quyền (bao gồm bản quyền thương mại hoặc mã nguồn mở có nguồn gốc rõ ràng), các dịch vụ cài đặt trên máy chủ là các dịch vụ được sử dụng dùng chung cho cơ quan, đơn vị, không cài đặt các dịch vụ không sử dụng.

b) Thiết lập chế độ tự động cập nhật bản vá hệ điều hành, phần mềm, ứng dụng và hệ quản trị cơ sở dữ liệu được cài đặt trên máy chủ, phải thiết lập mật khẩu truy nhập chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng đối với tất cả máy chủ.

c) Các máy chủ cần được cài đặt mật khẩu ở phần cấu hình (setup) của BIOS, trong đó lưu ý việc vô hiệu hóa các cổng USB trên máy chủ.

d) Không sử dụng thiết bị lưu trữ cá nhân để sao chép, lưu trữ thông tin, dữ liệu của cơ quan; khi cần khôi phục dữ liệu trong trên máy chủ, máy tính trạm của cơ quan bị hư hỏng, đơn vị quản lý thông báo Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ.

2. Cơ quan chủ quản có trách nhiệm trang bị phần mềm phòng chống mã độc (antivirus) cho hệ thống máy chủ; đơn vị vận hành thiết lập chế độ tự động cập nhật phiên bản mới, các bản vá lỗi; chế độ tự động quét mã độc khi sao chép, mở các tập tin; chế độ quét toàn bộ máy tính định kỳ hàng tuần.

3. Định kỳ hàng tuần đơn vị vận hành phải kiểm tra các tiến trình trên máy chủ nhằm sớm phát hiện nguy cơ cài cắm phần mềm độc hại trên máy chủ.

4. Quản lý logfile: Đơn vị vận hành phải thường xuyên kiểm tra, quản lý, sao lưu các logfile theo từng tháng, thời gian lưu trữ logfile trên máy chủ và thiết bị từ 06 - 12 tháng, các tập tin logfile cũ trong 03 năm trước đó cần được lưu trữ trên các ổ cứng ngoài; định kỳ 6 tháng thiết bị giám sát bảo đảm tính toàn vẹn của các logfile, hạn chế tình trạng tràn logfile gây ảnh hưởng đến hoạt động của HTTT.

5. Quản lý lưu ký hệ thống: Việc thực hiện lưu ký HTTT yêu cầu đơn vị cung cấp dịch vụ lưu ký phải tổ chức máy chủ cơ sở dữ liệu và máy chủ ứng dụng nằm trên hai máy chủ khác nhau và được bảo vệ bởi lớp bảo vệ bao gồm: tường lửa, thiết bị phòng chống tấn công từ chối dịch vụ DDoS (Distributed Denial of Service), thiết bị phát hiện và phòng chống xâm nhập trái phép (IPS/IDS),...

6. Quản lý phiên bản: Đơn vị vận hành xây dựng nhật ký quản lý phiên bản

HTTT bao gồm các thông tin: Chủ đầu tư, Tên HTTT, đơn vị phát triển, tên phiên bản; các chức năng của phiên bản; các chức năng thay đổi so với phiên bản trước, thời gian thay đổi; lưu trữ các phiên bản HTTT tại hệ thống lưu trữ độc lập.

7. Khi thiết lập cung cấp các dịch vụ ra môi trường mạng (tuân thủ theo TCP/UDP Port), đơn vị vận hành yêu cầu nhà cung cấp dịch vụ cấu hình trên máy chủ ứng dụng những dịch vụ thiết yếu nhất để bảo đảm hoạt động của hệ thống, không kích hoạt những chức năng, cổng giao tiếp mạng, giao thức và các dịch vụ không sử dụng (không thiết lập cấu hình các dịch vụ ra môi trường mạng đối với máy chủ cơ sở dữ liệu).

8. Nghiêm cấm sử dụng các tài nguyên tính toán như: các máy chủ và các cổng dịch vụ môi trường mạng để xây dựng các hệ thống thực hiện các hành vi đào tiền ảo, rà quét các lỗ hổng bảo mật, hoặc tham gia các hoạt động bất hợp pháp khác trên môi trường mạng.

Điều 7. Bảo đảm an toàn dữ liệu

1. Quản lý tài khoản và chữ ký số

a) Khi cấp tài khoản, chữ ký số lần đầu cho người dùng truy nhập, đơn vị vận hành phải thông báo (qua email, điện thoại,...) và người dùng phải thay đổi mật khẩu sau khi đăng nhập thành công lần đầu. Sau thời gian chậm nhất là 03 ngày, các tài khoản không tuân thủ việc thay đổi mật khẩu các tài khoản của các HTTT tự động vô hiệu hóa.

b) Các HTTT khi phân quyền phải thiết lập chế độ giới hạn số lần đăng nhập không hợp lệ vào hệ thống tối đa không quá 05 lần, khi người dùng đăng nhập sai vượt quá số lần quy định, tài khoản chuyển sang chế độ khóa quyền truy cập; các HTTT xác lập chế độ thoát ra khỏi hệ thống nếu người sử dụng không tương tác trên hệ thống của phiên làm việc quá 10 phút.

c) Chủ tài khoản, chữ ký số không chia sẻ, giao quyền tài khoản, chữ ký số và mật khẩu truy nhập cho người khác. Không sử dụng tài khoản của người khác (tài khoản thư điện tử, chữ ký số, chứng thư số...) để đăng nhập vào HTTT, cơ sở dữ liệu.

d) Tài khoản thư điện tử, chữ ký số chuyên dùng (xxx@danang.gov.vn và chữ ký số do Ban Cơ yếu Chính phủ cấp) là tài khoản để phục vụ cho các hoạt động mang tính công vụ, không sử dụng để giao dịch, đăng ký trên mạng xã hội, các trang thông tin điện tử công cộng khác.

đ) Khi cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc, nghỉ hưu, ngay từ thời điểm Quyết định có hiệu lực, đơn vị quản lý cá nhân đó phải thông báo đơn vị vận hành để điều chỉnh, thu hồi, hủy bỏ tài khoản, chữ ký số, chứng thư số,...

e) Tài khoản quản trị hệ thống là tài khoản được giao cho cán bộ chuyên trách CNTT phục vụ cho công tác quản trị, phân quyền, cấu hình hệ thống đó Cán bộ quản trị hệ thống không sử dụng cùng một mật khẩu cho nhiều tài khoản khác nhau.

g) Khi cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc, nghỉ hưu,

ngay từ thời điểm thay đổi có hiệu lực, đơn vị quản lý cá nhân đó phải thông báo đơn vị vận hành để điều chỉnh, thu hồi, hủy bỏ tài khoản và các tài sản liên quan (khóa, thẻ nhận dạng, chữ ký số,...).

2. Các đơn vị khi triển khai dịch vụ sao lưu dự phòng ở mức vật lý cần thiết lập chức năng RAID (Redundant Arrays of Inexpensive Disks hoặc Redundant Arrays of Independent Disks) để tăng tốc độ đọc ghi hoặc bảo đảm khả năng lưu trữ dự phòng. Các đơn vị khi thuê dịch vụ cần yêu cầu nhà cung cấp dịch vụ thiết lập các giải pháp sao lưu tự động đối với dữ liệu trên máy chủ cơ sở dữ liệu và máy chủ ứng dụng và xây dựng các kịch bản có sẵn để khôi phục lại toàn bộ máy chủ hoặc các tập tin, thư mục khi xảy ra sự cố.

3. Đơn vị vận hành, các tổ chức cung cấp dịch vụ phải xây dựng nhật ký về quá trình sao lưu dữ liệu, thay đổi cấu trúc CSDL: Nội dung thay đổi, lý do thay đổi, thời gian, vị trí thay đổi,...; phân quyền đối với các thao tác thay đổi cấu trúc CSDL (tạo CSDL, tạo bảng, thay đổi cấu trúc bảng...); việc thay đổi, hủy,... chữ ký số tuân thủ các quy định pháp luật về chữ ký số.

4. Các tên miền (bao gồm cả tên miền xxx.danang.gov.vn) khi không còn sử dụng có văn bản gửi đến Sở Thông tin và Truyền thông và Trung Tâm Internet Việt Nam (VNNIC) để đề nghị hủy tên miền; các HTTT không sử dụng, chủ quản HTTT thực hiện việc thu hồi máy chủ, thu hồi ứng dụng và thực hiện việc lưu trữ dữ liệu ra thiết bị lưu trữ ngoài và yêu cầu đơn vị cung cấp dịch vụ lưu ký xóa hoàn toàn dữ liệu trên các máy chủ.

5. Khi thực hiện chia sẻ tài nguyên trên máy chủ hoặc máy trạm, đơn vị vận hành phải sử dụng mật khẩu để bảo vệ thông tin, dữ liệu; không thực hiện chia sẻ toàn bộ ổ cứng; theo dõi, giám sát để kết thúc chia sẻ tài nguyên ngay khi hoàn thành.

6. Đơn vị quản lý máy chủ, máy trạm và thiết bị lưu trữ khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài cơ quan phải tháo rời bộ phận lưu trữ khỏi thiết bị và để lại cơ quan, hoặc xóa dữ liệu lưu trữ trên thiết bị. Khi thanh lý thiết bị phải xóa dữ liệu lưu trữ bằng phần mềm hoặc thiết bị hủy dữ liệu chuyên dụng.

7. Thông tin, dữ liệu thuộc phạm vi bí mật nhà nước phải được quản lý theo quy định hiện hành về bảo vệ bí mật nhà nước.

Điều 8. Bảo đảm an toàn thiết bị và người dùng đầu cuối

1. Cá nhân khi sử dụng máy tính, thiết bị đầu cuối cài đặt Hệ điều hành là phần mềm có bản quyền (bao gồm bản quyền thương mại hoặc mã nguồn mở có nguồn gốc rõ ràng); thiết lập chế độ tự động cập nhật bản vá hệ điều hành trên máy tính, phải thiết lập mật khẩu truy nhập chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng; các máy tính cần được cài đặt mật khẩu ở phần cấu hình (setup) của BIOS, trong đó lưu ý việc vô hiệu hóa các cổng USB.

2. Trên máy tính cá nhân, sử dụng những trình duyệt an toàn, đáng tin cậy, cài đặt phần mềm phòng chống mã độc, tắt tính năng lưu mật khẩu tự động; thiết lập chế độ tự động cập nhật phần mềm phòng chống mã độc, chế độ tự động rà quét mã độc

khi sao chép, mở các tập tin, chế độ rà quét máy tính định kỳ hàng tuần.

3. Cá nhân khi mang thiết bị CNTT (máy tính, thiết bị di động) thuộc sở hữu riêng đến cơ quan và kết nối với mạng nội bộ để xử lý công việc phải được sự đồng ý của thủ trưởng cơ quan, đơn vị. Các thiết bị cá nhân này phải tuân thủ Điều 8 Quy chế này.

4. Cá nhân khi sử dụng máy tính, thiết bị đầu cuối được kết nối trong mạng nội bộ cơ quan và sử dụng để xử lý công việc mang tính chất công vụ phải tuân thủ các quy định sau:

a) Chỉ truy nhập vào các trang thông tin điện tử (website) tin cậy. Không truy cập vào các đường dẫn, tập tin không rõ nguồn gốc qua thư điện tử hoặc các đường liên kết chia sẻ trên các trang mạng xã hội, tin nhắn của các ứng dụng OTT như Zalo, Viber, Facetime,...

b) Thiết lập mật khẩu có độ phức tạp cao, không lưu trữ tài khoản trên máy tính, sử dụng chức năng mã hóa ở mức hệ điều hành bảo đảm các dữ liệu các tập tin văn bản,... được mã hóa trước khi truyền trên môi trường mạng.

c) Không sử dụng máy tính cá nhân được cơ quan cấp để kết nối Internet tại các điểm truy cập Internet công cộng để xử lý công vụ. Không sử dụng thư điện tử cá nhân từ hệ thống thư điện tử công cộng (Gmail, Yahoo,...) để trao đổi, gửi, nhận văn bản công vụ.

d) Khi phát hiện dấu hiệu máy tính nhiễm mã độc (máy chạy chậm bất thường, cảnh báo từ phần mềm antivirus, mất dữ liệu, xuất hiện các tập tin lạ,...), lập tức tắt máy và thông báo cán bộ chuyên trách CNTT để xử lý.

Điều 9. Sử dụng mạng xã hội an toàn

CBCCVC-NLĐ làm việc tại các cơ quan thuộc UBND thành phố Đà Nẵng khi sử dụng mạng xã hội thực hiện các biện pháp bảo đảm an toàn như sau:

1. Nghiêm cấm cung cấp, tiết lộ, đăng tải thông tin, dữ liệu của cơ quan nhà nước trên mạng xã hội, đặc biệt là các thông tin thuộc nội dung bí mật nhà nước.

2. Nghiêm cấm việc sử dụng mạng xã hội để chống lại Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội; phá hoại khối đại đoàn kết dân tộc; tuyên truyền chiến tranh, khủng bố; gây hận thù, mâu thuẫn giữa các dân tộc, sắc tộc, tôn giáo; tuyên truyền, kích động bạo lực, dâm ô, đồi trụy, tội ác, tệ nạn xã hội, mê tín dị đoan, phá hoại thuần phong, mỹ tục của dân tộc.

3. Nghiêm cấm phát tán trên mạng xã hội các thông tin giả mạo, sai sự thật, xuyên tạc, vu khống, xúc phạm uy tín của tổ chức, danh dự và nhân phẩm của cá nhân; xâm hại đến quyền và lợi ích hợp pháp của tổ chức, cá nhân.

4. Thiết lập chế độ quyền riêng tư và tắt chế độ định vị khi chia sẻ các thông tin cá nhân, bài viết trên mạng xã hội; kiểm soát các góp ý, thảo luận (comment) tránh để các tổ chức, cá nhân lợi dụng việc góp ý, bình luận, thảo luận để vi phạm các khoản 1,

khoản 2 và khoản 3 Điều này.

Chương III
QUẢN LÝ THIẾT KẾ, XÂY DỰNG, VẬN HÀNH HỆ THỐNG THÔNG TIN

Điều 10. Quản lý thiết kế, xây dựng hệ thống thông tin

1. Bảo đảm ATTT là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục trong suốt quá trình thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ HTTT; được thực hiện một cách đồng bộ, đầu tư tập trung, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng thiết bị, hiệu quả đầu tư.

2. Khi thiết kế xây dựng, nâng cấp, mở rộng HTTT, chủ quản HTTT phải xây dựng phương án bảo đảm ATTT trong hồ sơ thiết kế và gửi Sở Thông tin và Truyền thông thẩm định trước khi trình cấp có thẩm quyền phê duyệt dự án.

3. Đánh giá, phân loại cấp độ ATTT của HTTT:

a) Chủ quản HTTT có trách nhiệm tổ chức đánh giá, phân loại cấp độ ATTT của HTTT theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống theo cấp độ (gọi tắt là Nghị định số 85/2016/NĐ-CP) để áp dụng phương án bảo đảm ATTT phù hợp.

b) Hồ sơ đề xuất cấp độ lập theo hướng dẫn tại Điều 15 Nghị định số 85/2016/NĐ-CP, gửi Sở Thông tin và Truyền thông thẩm định, trình cấp có thẩm quyền phê duyệt.

c) Đối với HTTT được xây dựng mới hoặc nâng cấp, mở rộng, việc thẩm định phương án bảo đảm ATTT và hồ sơ đề xuất cấp độ ATTT thực hiện đồng thời với thẩm định dự án ứng dụng CNTT.

4. Trước khi đưa vào vận hành, khai thác HTTT, chủ quản HTTT phối hợp với tổ chức chuyên môn có đủ năng lực (đơn vị sự nghiệp nhà nước có chức năng, nhiệm vụ phù hợp hoặc tổ chức chuyên môn được cơ quan có thẩm quyền cấp phép theo Nghị định số 108/2016/NĐ-CP ngày 01/7/2016 của Chính phủ quy định chi tiết điều kiện kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng - gọi tắt là Nghị định số 108/2016/NĐ-CP) thực hiện đánh giá, kiểm định ATTT. Trên cơ sở đề xuất của đơn vị kiểm định, chủ quản HTTT có trách nhiệm tổ chức triển khai hiệu chỉnh thiết kế, mã nguồn để hạn chế, phòng ngừa rủi ro, nguy cơ xảy ra mất ATTT.

Điều 11. Quản lý thuê dịch vụ công nghệ thông tin

1. Khi ký kết hợp đồng thuê dịch vụ CNTT, cơ quan sử dụng dịch vụ phải xác định rõ phạm vi, trách nhiệm, quyền hạn và nghĩa vụ của các bên về bảo đảm ATTT. Trong hợp đồng phải bao gồm các điều khoản về việc xử lý vi phạm quy định bảo đảm ATTT và trách nhiệm bồi thường thiệt hại do hành vi vi phạm của bên cung cấp dịch vụ gây ra.

2. Trong quá trình sử dụng dịch vụ CNTT, cơ quan sử dụng dịch vụ có trách nhiệm:

a) Quản lý thông tin, dữ liệu phát sinh từ dịch vụ đó, không để bên cung cấp dịch vụ truy nhập, sử dụng thông tin, dữ liệu thuộc phạm vi nhà nước quản lý;

b) Yêu cầu bên cung cấp dịch vụ phải bảo mật thông tin, dữ liệu, mã nguồn, tài liệu thiết kế; triển khai các biện pháp bảo đảm ATTT theo quy định tại Quy chế này, Luật An toàn thông tin mạng và các quy định khác có liên quan;

c) Giám sát chặt chẽ và giới hạn quyền truy cập của bên cung cấp dịch vụ khi cho phép truy cập vào HTTT của cơ quan.

3. Khi phát hiện bên cung cấp dịch vụ có dấu hiệu vi phạm quy định bảo đảm ATTT, cơ quan sử dụng dịch vụ phải:

a) Tạm dừng hoặc đình chỉ hoạt động của bên cung cấp dịch vụ tùy theo mức độ vi phạm.

b) Thông báo chính thức các hành vi vi phạm của bên cung cấp dịch vụ.

c) Thu hồi ngay lập tức quyền truy cập HTTT đã cấp cho bên cung cấp dịch vụ.

d) Kiểm tra, xác định, lập báo cáo mức độ vi phạm và thiệt hại xảy ra; thông báo cho bên cung cấp dịch vụ và tiến hành các thủ tục xử lý vi phạm và bồi thường thiệt hại.

4. Sau khi kết thúc công việc, cơ quản sử dụng dịch vụ có trách nhiệm:

a) Thu hồi quyền truy cập HTTT và các tài sản khác liên quan đã cấp cho bên cung cấp dịch vụ; thay đổi các khóa, mật khẩu truy cập HTTT.

b) Yêu cầu bên cung cấp dịch vụ chuyển giao đầy đủ các thông tin, dữ liệu, mã nguồn, tài liệu thiết kế và các công cụ cần thiết để bảo đảm cơ quan vẫn có thể khai thác sử dụng dịch vụ được liên tục kể cả trong trường hợp thay đổi bên cung cấp dịch vụ.

Điều 12. Giám sát an toàn hệ thống thông tin

1. Các HTTT thuộc Danh mục HTTT quan trọng của thành phố Đà Nẵng là đối tượng bắt buộc giám sát ATTT.

2. Đối với các HTTT, phần mềm, ứng dụng, cơ sở dữ liệu được lưu ký tại trung tâm dữ liệu/hệ thống máy chủ riêng của cơ quan hoặc lưu ký tại doanh nghiệp ngoài, chủ quản HTTT có trách nhiệm tự thực hiện hoặc yêu cầu doanh nghiệp cung cấp dịch vụ lưu ký bảo đảm các yêu cầu giám sát an toàn HTTT tại Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin.

3. Sở Thông tin và Truyền thông có trách nhiệm tổ chức giám sát ATTT đối với các HTTT lưu ký tại Trung tâm dữ liệu thành phố Đà Nẵng.

4. Đơn vị vận hành thường xuyên giám sát hiệu năng hệ thống và thực hiện các biện pháp bảo trì cần thiết để bảo đảm khả năng xử lý và tính sẵn sàng của HTTT.

Điều 13. Kiểm tra, đánh giá rủi ro an toàn thông tin

1. Trong quá trình vận hành HTTT, chủ quản HTTT có trách nhiệm tổ chức kiểm tra, đánh giá rủi ro ATTT đối với HTTT do cơ quan mình quản lý.

2. Thời hạn thực hiện:

a) Đối với các HTTT thuộc Danh mục HTTT quan trọng của thành phố Đà Nẵng: thực hiện định kỳ hàng năm hoặc đột xuất theo đề nghị của Sở Thông tin và Truyền thông.

b) Đối với các HTTT khác: thực hiện định kỳ 02 năm/lần hoặc đột xuất theo đề nghị của Sở Thông tin và Truyền thông.

3. Trình tự thực hiện kiểm tra, đánh giá rủi ro ATTT:

a) Bước 1: Chủ quản HTTT xác định phạm vi, đối tượng, nội dung kiểm tra, đánh giá rủi ro ATTT, trong đó:

- Đối tượng kiểm tra, đánh giá bao gồm: hạ tầng mạng, hệ thống máy chủ, máy trạm, hệ thống lưu trữ, HTTT, phần mềm, ứng dụng, cơ sở dữ liệu, trang thông tin điện tử,...

- Nội dung kiểm tra, đánh giá bao gồm:

+ Kiểm tra việc tuân thủ các quy định của pháp luật về bảo đảm ATTT;

+ Đánh giá hiệu quả của phương án bảo đảm ATTT đang triển khai;

+ Đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm tấn công xâm nhập hệ thống và đánh giá nguy cơ, thiệt hại có thể có khi bị xâm nhập.

b) Bước 2: Lựa chọn đơn vị tư vấn đủ năng lực để triển khai kiểm tra, đánh giá rủi ro ATTT (đơn vị sự nghiệp nhà nước có chức năng, nhiệm vụ phù hợp hoặc tổ chức chuyên môn được cơ quan có thẩm quyền cấp phép theo Nghị định số 108/2016/NĐ-CP).

c) Bước 3: Đơn vị tư vấn xây dựng kế hoạch kiểm tra, đánh giá rủi ro ATTT (*theo Mẫu số 01 tại Phụ lục II kèm theo Quy chế này*), gửi Sở Thông tin và Truyền thông có ý kiến trước khi trình chủ quản HTTT phê duyệt.

d) Bước 4: Đơn vị tư vấn triển khai kiểm tra, đánh giá rủi ro ATTT trên cơ sở kế hoạch được phê duyệt.

đ) Bước 5: Đơn vị tư vấn lập báo cáo kết quả kiểm tra, đánh giá rủi ro ATTT (*theo Mẫu số 02 tại Phụ lục II kèm theo Quy chế này*), gửi Sở Thông tin và Truyền thông có ý kiến trước khi trình chủ quản HTTT phê duyệt.

e) Bước 6: Hồ sơ kiểm tra, đánh giá rủi ro ATTT phải được lưu trữ và gửi 01 bộ về Sở Thông tin và Truyền thông để theo dõi, tổng hợp.

Điều 14. Xử lý rủi ro an toàn thông tin

Trên cơ sở báo cáo kết quả kiểm tra, đánh giá rủi ro ATTT hoặc khi tiếp nhận cảnh báo điểm yếu, lỗ hổng bảo mật tiềm ẩn nguy cơ gây mất ATTT từ Sở Thông tin

và Truyền thông, chủ quản HTTT có trách nhiệm thực hiện hoặc lựa chọn đơn vị đủ năng lực để triển khai các phương án xử lý. Khi hoàn thành xử lý, báo cáo kết quả xử lý về Sở Thông tin và Truyền thông để theo dõi, tổng hợp.

Điều 15. Ứng cứu xử lý sự cố an toàn thông tin

1. Nguyên tắc ứng cứu xử lý sự cố

a) Chủ động, kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả.

b) Phối hợp chặt chẽ, tuân thủ quy định của pháp luật về điều phối ứng cứu sự cố ATTT.

c) Ứng cứu xử lý sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản HTTT.

d) Việc xử lý sự cố ATTT phải bảo đảm quyền và lợi ích hợp pháp của cơ quan, cá nhân, bảo mật thông tin cá nhân, thông tin riêng của cơ quan khi tham gia các hoạt động ứng cứu xử lý sự cố.

2. Phân loại sự cố ATTT

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

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

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

d) Sự cố do các thảm họa tự nhiên.

3. Phân loại mức độ nghiêm trọng sự cố

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 tác động đến khả năng vận hành của HTTT, ảnh hưởng đến dữ liệu, thiết bị, gây ảnh hưởng đến hoạt động chung của cơ quan và hoạt động cung cấp dịch vụ công cho người dân, doanh nghiệp.

d) Nghiêm trọng: Sự cố gây gián đoạn hoặc đình trệ hệ thống trong một khoảng thời gian ngắn, ảnh hưởng nghiêm trọng đến dữ liệu, thiết bị của hệ thống, gây thiệt hại nghiêm trọng cho cơ quan, người dân, doanh nghiệp.

đ) Đặc biệt nghiêm trọng: Sự cố làm tê liệt toàn bộ hoạt động của hệ thống, gây thiệt hại đặc biệt nghiêm trọng cho cơ quan, người dân, doanh nghiệp, đe dọa trật tự an toàn xã hội.

4. Quy trình phối hợp ứng cứu xử lý sự cố

a) Bước 1: Tiếp nhận sự cố

Chủ quản HTTT, đơn vị vận hành tiếp nhận thông tin, cảnh báo về việc mất ATTT của hệ thống từ các đơn vị chuyên trách ATTT, từ người sử dụng hoặc tự rà soát, phát hiện hệ thống có hiện tượng bất thường, có nguy cơ mất ATTT.

b) Bước 2: Xác minh và phân loại sơ bộ sự cố

Đơn vị vận hành tiến hành xác minh, phân loại sơ bộ sự cố; đánh giá tình trạng, mức độ, phạm vi và khả năng xử lý của sự cố.

c) Bước 3: Báo cáo thông tin sự cố

- Trường hợp xác định sự cố nằm trong thẩm quyền, khả năng xử lý, đơn vị vận hành báo cáo lãnh đạo cơ quan chủ quản và thực hiện xử lý theo phương án ứng cứu xử lý sự cố nội bộ đã được phê duyệt hoặc theo hướng dẫn của Sở Thông tin và Truyền thông. Khi hoàn thành xử lý, báo cáo kết quả xử lý sự cố (*theo Mẫu số 04 tại Phụ lục II kèm theo Quy chế này*) về Sở Thông tin và Truyền thông để theo dõi, tổng hợp;

- Trường hợp xác định sự cố có mức độ cao, vượt ngoài thẩm quyền, khả năng xử lý, đơn vị vận hành lập tức báo cáo lãnh đạo cơ quan chủ quản và thông báo (qua điện thoại, email,...) đầu mối tiếp nhận sự cố của Sở Thông tin và Truyền thông để kịp thời phối hợp với Đội ứng cứu sự cố và các đơn vị chuyên trách ATTT. Ngay trong ngày xảy ra sự cố, đơn vị vận hành thực hiện báo cáo ban đầu sự cố ATTT (*theo Mẫu số 03 tại Phụ lục II kèm theo Quy chế này*) và gửi về Sở Thông tin và Truyền thông. Đơn vị vận hành có trách nhiệm phối hợp, hỗ trợ Đội ứng cứu sự cố thực hiện các bước ứng cứu xử lý sự cố tiếp theo.

d) Bước 4: Cách ly

Đội ứng cứu sự cố cách ly máy chủ, thiết bị, phân vùng bị sự cố ra khỏi môi trường mạng nhằm ngăn chặn khả năng lây lan của sự cố sang những máy chủ, thiết bị, phân vùng khác.

đ) Bước 5: Thu thập thông tin sự cố

Đội ứng cứu sự cố thu thập thông tin, phục vụ phân tích sự cố, bao gồm: Thông tin về đầu mối liên hệ; thông tin hệ thống; thông tin chức năng của hệ thống; thông tin cấu hình của hệ thống (hệ điều hành, dịch vụ, phiên bản, cấu trúc mạng...); thu thập chứng cứ, thông tin bộ nhớ, trạng thái mạng và các kết nối; tiến trình đang chạy, ổ cứng (trong và ngoại vi); thu thập logfile...

e) Bước 6: Phân tích sự cố

Đội ứng cứu sự cố tiến hành phân tích sự cố, bao gồm các thông tin sau: Phân tích dòng thời gian; thời gian bị sửa đổi, truy cập, tạo hoặc thay đổi; thời gian thực hiện các cập nhật lớn đối với hệ thống; thời điểm mà hệ thống sử dụng lần cuối cùng; phân tích dữ liệu; kiểm tra sự thay đổi cấu hình; kiểm tra hệ thống tập tin có bị mã độc; kiểm tra tập tin lịch sử Internet (Internet History) và các tập tin lịch sử khác; kiểm tra Registry và tiến trình; quan sát các tập tin, tiến trình lúc khởi động; phân tích logfile...

g) Bước 7: Xử lý sự cố

Đội ứng cứu sự cố xây dựng phương án xử lý sự cố, báo cáo xin ý kiến lãnh đạo Sở Thông tin và Truyền thông, chủ quản HTTT về phương án xử lý sự cố; tiến hành xử lý sự cố, bao gồm các bước: Gỡ bỏ sự cố; xác định và gỡ bỏ các backdoors; phân tích và kiểm tra lỗ hổng sau khi thực hiện các bản vá lỗi; khôi phục dữ liệu; thu thập các tập tin, hình ảnh, email,... bị xóa, thời gian bị xóa; tìm kiếm và khôi phục các tập tin phù hợp,... để khôi phục HTTT hoạt động bình thường trở lại.

h) Bước 8: Tổng hợp, báo cáo

Đội ứng cứu sự cố và đơn vị vận hành hệ thống tiến hành tổng hợp kết quả phân tích và xử lý sự cố, báo cáo với lãnh đạo Sở Thông tin và Truyền thông và chủ quản HTTT để tổ chức họp phân tích nguyên nhân, rút kinh nghiệm trong hoạt động xử lý sự cố và đề xuất các biện pháp phòng ngừa xảy ra sự cố tương tự. Chủ quản HTTT gửi báo cáo hoàn thành xử lý sự cố ATTT (*theo Mẫu số 04 tại Phụ lục II kèm theo Quy chế này*) về Sở Thông tin và Truyền thông tổng hợp.

i) Bước 9: Lưu hồ sơ

Các cơ quan, đơn vị tham gia ứng cứu sự cố lưu toàn bộ các hồ sơ trong quá trình xử lý sự cố để phục vụ các hoạt động quản lý và theo dõi định kỳ. Hồ sơ lưu trữ gồm: Báo cáo ban đầu sự cố; kế hoạch xử lý sự cố, hồ sơ xử lý sự cố, báo cáo phân tích kết quả điều tra xử lý sự cố, báo cáo hoàn thành xử lý sự cố.

Chương IV
TỔ CHỨC THỰC HIỆN

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

1. Thực hiện vai trò cơ quan chuyên trách ATTT của UBND thành phố Đà Nẵng và là thành viên Mạng lưới ứng cứu sự cố ATTT mạng quốc gia; có trách nhiệm tổ chức thực hiện các quy định, quy chế bảo đảm ATTT trên địa bàn thành phố Đà Nẵng; đầu mối điều phối, hướng dẫn ứng cứu xử lý sự cố ATTT trên địa bàn thành phố và tham gia các hoạt động ứng cứu sự cố khẩn cấp bảo đảm ATTT mạng quốc gia.

2. Tham mưu UBND thành phố Đà Nẵng ban hành các cơ chế, chính sách, kế hoạch, đề án bảo đảm ATTT trên địa bàn thành phố Đà Nẵng.

3. Chịu trách nhiệm quản lý, vận hành và bảo đảm ATTT đối với hệ thống hạ tầng kỹ thuật CNTT và HTTT chính quyền điện tử thành phố Đà Nẵng.

4. Rà soát, tổng hợp, tham mưu UBND thành phố Đà Nẵng điều chỉnh, bổ sung Danh mục HTTT quan trọng của thành phố Đà Nẵng.

5. Thẩm định phương án bảo đảm ATTT trong hồ sơ thiết kế HTTT và thẩm định hồ sơ đề xuất cấp độ ATTT của HTTT theo các quy định của pháp luật hiện hành.

6. Định kỳ tổ chức đào tạo, tập huấn nâng cao trình độ, kỹ năng nghiệp vụ bảo đảm ATTT cho các cán bộ chuyên trách CNTT trên địa bàn thành phố Đà Nẵng; tổ chức đào tạo, bồi dưỡng kiến thức, kỹ năng cơ bản về ATTT thông qua Cổng đào tạo trực tuyến cho CBCCVC-NLĐ của các cơ quan trên địa bàn thành phố.

7. Tuyên truyền, phổ biến nâng cao nhận thức về ATTT trong các cơ quan nhà nước và cộng đồng xã hội.

8. Định kỳ tổ chức diễn tập ứng cứu sự cố ATTT trên địa bàn thành phố, tham gia diễn tập quốc gia và quốc tế do Bộ Thông tin và Truyền thông tổ chức.

9. Phối hợp, liên kết với các cơ quan chuyên trách ATTT (Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam - VNCERT, Cục An toàn thông tin, Bộ Tư lệnh 86, Ban Cơ yếu Chính phủ) trong công tác giám sát, kiểm tra, đánh giá, xử lý sự cố ATTT, thường xuyên trao đổi thông tin, cảnh báo nguy cơ, điểm yếu, lỗ hổng bảo mật, các giải pháp, biện pháp bảo đảm ATTT.

10. Kịp thời cảnh báo cho các cơ quan và hướng dẫn xử lý các nguy cơ, điểm yếu, lỗ hổng bảo mật, sự cố ATTT.

11. Định kỳ hàng năm hoặc đột xuất tiến hành kiểm tra, đánh giá công tác bảo đảm ATTT trong hoạt động ứng dụng CNTT của các cơ quan; tổng hợp, báo cáo UBND thành phố Đà Nẵng. Trường hợp phát hiện các hành vi vi phạm, gây hậu quả nghiêm trọng, báo cáo UBND thành phố Đà Nẵng xem xét, xử lý.

12. Định kỳ hàng năm hoặc đột xuất tổng hợp, báo cáo UBND thành phố Đà Nẵng tình hình bảo đảm ATTT trên địa bàn thành phố Đà Nẵng.

13. Xây dựng dự toán kinh phí đầu tư nâng cấp, mở rộng hệ thống hạ tầng kỹ thuật ATTT và triển khai công tác bảo đảm ATTT trong nguồn kinh phí sự nghiệp CNTT hàng năm, gửi Sở Tài chính thẩm định, tổng hợp trong kế hoạch ngân sách thành phố, trình UBND thành phố Đà Nẵng phê duyệt.

Điều 17. Trách nhiệm của Công an thành phố Đà Nẵng

1. Chủ trì, phối hợp với Sở Thông tin và Truyền thông triển khai công tác bảo đảm ATTT bảo vệ bí mật nhà nước.

2. Kịp thời cảnh báo các phương thức, thủ đoạn mới của các loại tội phạm công nghệ cao; chịu trách nhiệm quản lý, kiểm soát, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống mạng gây hại đến ATTT của cơ quan, cá nhân.

3. Cử cán bộ tham gia đoàn kiểm tra, đánh giá công tác bảo đảm ATTT trong hoạt động ứng dụng CNTT của các cơ quan trên địa bàn thành phố; kiểm tra đột xuất khi có dấu hiệu vi phạm pháp luật về ATTT; tổ chức điều tra và xử lý các trường hợp vi phạm ATTT theo thẩm quyền và theo quy định của pháp luật.

Điều 18. Trách nhiệm của Sở Kế hoạch và Đầu tư và Sở Tài chính

1. Hàng năm, trên cơ sở khả năng cân đối ngân sách và chế độ, tiêu chuẩn, định mức theo quy định của Luật Ngân sách Nhà nước, Sở Tài chính có trách nhiệm tham mưu UBND thành phố Đà Nẵng bố trí kinh phí bảo đảm ATTT cho các cơ quan, đơn vị trên địa bàn thành phố.

2. Sở Kế hoạch và Đầu tư chủ trì, phối hợp với Sở Thông tin và Truyền thông tổng hợp, tham mưu ưu tiên bố trí nguồn vốn ngân sách trong kế hoạch chi đầu tư phát

triển hàng năm và kế hoạch vốn đầu tư công trung hạn để thực hiện các dự án đầu tư bảo đảm ATTT.

Điều 19. 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 bảo đảm ATTT tại Quy chế này và các quy định khác của pháp luật hiện hành; chịu trách nhiệm toàn diện trước UBND thành phố Đà Nẵng trong công tác bảo đảm ATTT tại đơn vị mình.

2. Căn cứ Quy chế này và chức năng, nhiệm vụ đặc thù của cơ quan, thực hiện xây dựng hoặc rà soát sửa đổi Quy chế bảo đảm ATTT và Kế hoạch ứng phó sự cố ATTT nội bộ cho phù hợp.

3. Thường xuyên rà soát, đề xuất Sở Thông tin và Truyền thông bổ sung vào Danh mục HTTT quan trọng của thành phố Đà Nẵng.

4. Tổ chức xây dựng hồ sơ đề xuất cấp độ ATTT đối với HTTT do cơ quan quản lý, vận hành, gửi Sở Thông tin và Truyền thông thẩm định, trình cấp có thẩm quyền phê duyệt.

5. Tổ chức giám sát ATTT, kiểm tra, đánh giá, xử lý rủi ro ATTT đối với HTTT thuộc Danh mục HTTT quan trọng của thành phố Đà Nẵng.

6. Phối hợp, cung cấp thông tin và tạo điều kiện để Đội ứng cứu sự cố triển khai công tác xử lý, khắc phục sự cố nhanh chóng, kịp thời, hiệu quả.

7. Phối hợp chặt chẽ với Sở Thông tin và Truyền thông và Công an thành phố Đà Nẵng trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm ATTT.

8. Thường xuyên tuyên truyền, phổ biến nâng cao nhận thức về ATTT, đào tạo, hướng dẫn các kiến thức, kỹ năng cơ bản về ATTT cho CBCCVC-NLĐ của đơn vị mình.

9. Hàng năm bố trí kinh phí từ nguồn kinh phí thường xuyên của cơ quan để đầu tư mua sắm hệ điều hành, phần mềm có bản quyền, thiết bị phòng vệ chuyên dụng.

10. Định kỳ 06 tháng (trước ngày 15/7) và hàng năm (trước ngày 15/01 năm tiếp theo) báo cáo tình hình ATTT của cơ quan (*theo Mẫu số 05 tại Phụ lục kèm theo Quy chế này*), gửi Sở Thông tin và Truyền thông tổng hợp.

Điều 20. Trách nhiệm của đơn vị vận hành hệ thống thông tin

1. Thực hiện các biện pháp bảo đảm ATTT theo quy định tại Quy chế này và các quy định khác của pháp luật có liên quan; tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật về ATTT.

2. Xây dựng hồ sơ đề xuất cấp độ, trình thẩm định, phê duyệt theo quy định.

3. Định kỳ đánh giá hiệu quả các biện pháp bảo đảm ATTT, báo cáo chủ quản HTTT điều chỉnh nếu cần thiết.

4. Định kỳ hoặc đột xuất báo cáo công tác thực hiện bảo đảm ATTT theo yêu cầu của chủ quản HTTT hoặc Sở Thông tin và Truyền thông.

5. Kịp thời thông báo sự cố ATTT và phối hợp ứng cứu xử lý sự cố ATTT với các cơ quan, đơn vị liên quan.

Điều 21. Trách nhiệm của cán bộ, công chức, viên chức, người lao động trong cơ quan, đơn vị

1. Trách nhiệm cán bộ chuyên trách CNTT

a) Phụ trách công tác bảo đảm ATTT tại cơ quan, đơn vị.

b) Tham mưu thủ trưởng cơ quan, đơn vị ban hành các quy định, quy trình nội bộ, triển khai các biện pháp bảo đảm ATTT theo Quy chế này và các quy định khác của pháp luật hiện hành.

c) Hỗ trợ, hướng dẫn tất cả CBCCVC-NLĐ trong cơ quan thực hiện các kỹ năng sử dụng máy tính an toàn.

d) Giám sát, đánh giá, báo cáo Thủ trưởng cơ quan kịp thời các rủi ro mất ATTT và mức độ nghiêm trọng của các rủi ro đó.

đ) Đầu mối phối hợp với Sở Thông tin và Truyền thông tiếp nhận cảnh báo các nguy cơ, điểm yếu, lỗ hổng bảo mật; cung cấp thông tin và phối hợp ứng cứu xử lý sự cố ATTT.

e) Tham gia đầy đủ các lớp đào tạo, bồi dưỡng kiến thức, kỹ năng chuyên sâu về ATTT, diễn tập ứng cứu sự cố ATTT do Sở Thông tin và Truyền thông hoặc các cơ quan chuyên trách ATTT tổ chức.

g) Thường xuyên cập nhật nâng cao kiến thức, trình độ chuyên môn đáp ứng yêu cầu bảo đảm ATTT tại cơ quan, đơn vị.

2. Trách nhiệm của CBCCVC-NLĐ

a) Chấp hành nghiêm túc các quy định, quy trình nội bộ của cơ quan, đơn vị, các quy định tại Quy chế này và các quy định khác của pháp luật hiện hành về bảo đảm ATTT.

b) Tự quản lý, bảo quản thiết bị mà mình được giao sử dụng. Thường xuyên cập nhật, nâng cao kỹ năng sử dụng máy tính an toàn.

c) Khi phát hiện sự cố mất ATTT phải thông báo ngay với cán bộ chuyên trách CNTT để kịp thời ngăn chặn, xử lý, khắc phục.

d) Tham gia nghiêm túc các chương trình đào tạo, bồi dưỡng về ATTT do cơ quan chủ quản hoặc Sở Thông tin và Truyền thông tổ chức.

Điều 22. Tổ chức thực hiện

Sở Thông tin và Truyền thông chủ trì, phối hợp với các sở, ban, ngành; UBND các quận, huyện, phường, xã và các cơ quan, đơn vị có liên quan triển khai thực hiện Quy chế này.

Trong quá trình thực hiện nếu có phát sinh khó khăn, vướng mắc hoặc cần sửa đổi, bổ sung; các cơ quan kịp thời báo cáo về Sở Thông tin và Truyền thông tổng hợp, trình UBND thành phố xem xét, quyết định./.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH
Huỳnh Đức Thơ

Phụ lục I
DANH MỤC HỆ THỐNG THÔNG TIN QUAN TRỌNG
CỦA THÀNH PHỐ ĐÀ NẴNG

(Ban hành kèm theo Quyết định số: 4159 /QĐ-UBND ngày 14 tháng 9 năm 2018 của Ủy ban nhân dân thành phố Đà Nẵng)

STT	Hệ thống thông tin	Cơ quan quản lý
1	Hạ tầng CNTT (Mạng MAN thành phố; Trung tâm dữ liệu thành phố; Hệ thống mạng không dây công cộng; Hệ thống tổng đài thông tin dịch vụ công; Hệ thống đào tạo trực tuyến; Hệ thống hội nghị trực tuyến và điện thoại IP phone,...)	Sở Thông tin và Truyền thông
2	HTTT chính quyền điện tử với các ứng dụng dùng chung tích hợp trên Hệ thống (Phần mềm Một cửa điện tử, phần mềm Quản lý văn bản và điều hành, hệ thống thư điện tử, dịch vụ công trực tuyến,...)	Sở Thông tin và Truyền thông
3	Cơ sở dữ liệu	
A	Cơ sở dữ liệu đất đai, bản đồ nền địa lý	Sở Tài nguyên và Môi trường
B	Cơ sở dữ liệu công dân, cơ sở dữ liệu nhân hộ khẩu	Sở Thông tin và Truyền thông
C	Cơ sở dữ liệu doanh nghiệp	Sở Kế hoạch và Đầu tư
4	Cổng thông tin điện tử thành phố Đà Nẵng	Văn phòng UBND thành phố Đà Nẵng
5	HTTT cơ sở dữ liệu chuyên ngành (hệ thống, phần mềm, cơ sở dữ liệu quản lý nhà nước chuyên ngành, trang thông tin điện tử,...)	Theo cơ quan quản lý chuyên ngành

Phụ lục II

DANH MỤC BIỂU MẪU

(Ban hành kèm theo Quyết định số: 4159/QĐ-UBND ngày 14 tháng 9 năm 2018 của Ủy ban nhân dân thành phố Đà Nẵng)

Mẫu số 01	Kế hoạch kiểm tra, đánh giá rủi ro an toàn thông tin
Mẫu số 02	Báo cáo kết quả kiểm tra, đánh giá rủi ro an toàn thông tin
Mẫu số 03	Báo cáo ban đầu sự cố an toàn thông tin
Mẫu số 04	Báo cáo hoàn thành xử lý sự cố an toàn thông tin
Mẫu số 05	Báo cáo định kỳ tình hình an toàn thông tin

(Mẫu số 01)

TÊN CƠ QUAN CHỦ QUẢN **TÊN CƠ QUAN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: ……/KH-	*Đà Nẵng, ngày ... tháng ... năm ...*

KẾ HOẠCH KIỂM TRA, ĐÁNH GIÁ RỦI RO AN TOÀN THÔNG TIN

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

2. Yêu cầu

II. PHẠM VI, ĐỐI TƯỢNG KIỂM TRA, ĐÁNH GIÁ

1. Phạm vi

(Mô tả phạm vi kiểm tra, đánh giá bao gồm các phòng, ban, đơn vị trực thuộc của cơ quan, đơn vị vận hành hệ thống, đơn vị cung cấp dịch vụ lưu ký, đơn vị thiết kế xây dựng hệ thống,…)

2. Đối tượng

Đối tượng kiểm tra, đánh giá bao gồm: hạ tầng mạng, hệ thống máy chủ, máy trạm, hệ thống lưu trữ, HTTT, phần mềm, ứng dụng, cơ sở dữ liệu, trang thông tin điện tử,...

III. NỘI DUNG KIỂM TRA, ĐÁNH GIÁ

1. Kiểm tra việc tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin

(Các quy định về quản lý phòng máy chủ, hạ tầng mạng, mạng không dây, quản lý tài khoản, quản lý đăng nhập, quản lý logfile, quản lý lưu ký, quản lý dữ liệu,....)

2. Đánh giá hiệu quả của phương án bảo đảm an toàn thông tin đang triển khai

3. Đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm tấn công xâm nhập hệ thống và phân tích, xác định mức độ rủi ro

IV. TIÊU CHÍ, PHƯƠNG PHÁP KIỂM TRA, ĐÁNH GIÁ

1. Tiêu chí

a) Tiêu chí đánh giá tác động rủi ro (nhằm xác định khả năng xảy ra, mức độ nghiêm trọng, hậu quả của các nguy cơ, mối đe dọa, điểm yếu ATTT)

b) Tiêu chí xác định mức độ ưu tiên xử lý rủi ro

2. Phương pháp

a) Phương pháp đánh giá định tính

b) Phương pháp đánh giá định lượng

V. TỔ CHỨC THỰC HIỆN

1. Phân công nhiệm vụ

2. Thời gian thực hiện

3. Kinh phí thực hiện và nguồn kinh phí

Nơi nhận:
- UBND thành phố;
- Sở Thông tin và Truyền thông;
- Các phòng, đơn vị;
- Lưu: VT,....

THỦ TRƯỞNG CƠ QUAN
(Ký số)

***Lưu ý**: Tham khảo Tiêu chuẩn Việt Nam TCVN 10295:2014 Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý rủi ro an toàn thông tin.*

(Mẫu số 02)

TÊN CƠ QUAN CHỦ QUẢN
TÊN CƠ QUAN
Số: ……/BC-

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc
Đà Nẵng, ngày ... tháng ... năm ...

BÁO CÁO KẾT QUẢ KIỂM TRA, ĐÁNH GIÁ RỦI RO AN TOÀN THÔNG TIN

I. CƠ SỞ PHÁP LÝ

II. QUÁ TRÌNH TỔ CHỨC THỰC HIỆN

III. KẾT QUẢ KIỂM TRA, ĐÁNH GIÁ

1. Kết quả kiểm tra việc tuân thủ các quy định và mức độ hiệu quả biện pháp bảo đảm an toàn thông tin

STT	Nội dung quy định	Tuân thủ		Mức độ đáp ứng		Ghi chú
		Có	Không	Có	Không	
I	**CHÍNH SÁCH, QUẢN LÝ**					
1	Xây dựng Quy chế bảo đảm ATTT nội bộ					
2	Xây dựng Kế hoạch ứng phó sự cố ATTT					
3	Xây dựng hồ sơ đề xuất cấp độ					Ghi rõ số lượng HTTT chưa được phe duyệt cấp độ trên tổng số HTTT hiện có
4	Thực hiện kiểm định ATTT đối với HTTT trước khi đưa vào vận hành					
5	Thực hiện các biện pháp xử lý rủi ro theo kết quả kiểm định					Ghi rõ mức độ thực hiện
6	Thực hiện giám sát ATTT					Ghi rõ phương pháp giám sát
7	Định kỳ thực hiện kiểm tra, đánh giá rủi ro ATTT					
8	Thực hiện các biện pháp xử lý rủi ro theo kết quả đánh					Ghi rõ mức độ thực hiện

	giá					
9	Định kỳ báo cáo tình hình ATTT					
10	Tổ chức đào tạo, tập huấn nâng cao kỹ năng, nhận thức ATTT					
11	Tham gia diễn tập ứng cứu sự cố ATTT					
II	**CÁC BIỆN PHÁP QUẢN LÝ KỸ THUẬT**					
1	Bảo đảm ATTT mức vật lý					
	…					
2	Bảo đảm an toàn hạ tầng mạng					
	…					
3	Bảo đảm an toàn máy chủ và ứng dụng					
	…					
4	Bảo đảm an toàn dữ liệu					
5	Bảo đảm an toàn thiết bị đầu cuối					
	…					

2. Phát hiện, đánh giá, phân tích rủi ro

STT	Nội dung rủi ro	Mức độ rủi ro	Khả năng xảy ra

3. Danh sách thứ tự ưu tiên xử lý rủi ro và biện pháp xử lý

IV. KẾT LUẬN, KIẾN NGHỊ

Nơi nhận:
- UBND thành phố;
- Sở Thông tin và Truyền thông;
- Các phòng, đơn vị;
- Lưu: VT,....

THỦ TRƯỞNG CƠ QUAN
(Ký số)

***Lưu ý**: Tham khảo Tiêu chuẩn Việt Nam TCVN 10295:2014 Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý rủi ro an toàn thông tin.*

(Mẫu số 03)

TÊN CƠ QUAN CHỦ QUẢN **TÊN CƠ QUAN** Số: …../BC-	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc** *Đà Nẵng, ngày ... tháng ... năm ...*

BÁO CÁO BAN ĐẦU SỰ CỐ AN TOÀN THÔNG TIN

THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN BÁO CÁO SỰ CỐ

- Tên tổ chức/cá nhân báo cáo sự cố (*) .....
- Địa chỉ: (*) .....
- Điện thoại (*)..... Email (*) .....

NGƯỜI LIÊN HỆ

- Họ và tên (*) ..... Chức vụ: .....
- Điện thoại (*)..... Email (*).....

THÔNG TIN CHI TIẾT VỀ HỆ THỐNG BỊ SỰ CỐ

Tên đơn vị vận hành HTTT (*):	*Điền tên đơn vị vận hành hoặc được thuê vận hành HTTT*				
Cơ quan chủ quản:	*Điền tên cơ quan chủ quản*				
Tên hệ thống bị sự cố	*Điền tên hệ thống bị sự cố và tên miền, địa chỉ ip liên quan*				
Phân loại cấp độ của HTTT, (nếu có)	☐ Cấp độ 1	☐ Cấp độ 2	☐ Cấp độ 3	☐ Cấp độ 4	☐ Cấp độ 5
Tổ chức cung cấp dịch vụ an toàn thông tin (nếu có):	*Điền tên nhà cung cấp ở đây*				
Tên nhà cung cấp dịch vụ kết nối bên ngoài (nếu có)	*Điền tên nhà cung cấp ở đây*				
Dải địa chỉ Public IP kết nối với hệ thống bên ngoài:	*Điền thông tin ở đây*				
Mô tả sơ bộ về sự cố (*)					
Đề nghị cung cấp một bản tóm tắt ngắn gọn về sự cố, bao gồm đánh giá sơ bộ cuộc tấn công đã xảy ra chưa và bất kỳ các nguy cơ dẫn đến khả năng phá hoại hoặc gián đoạn dịch vụ. Cũng vui lòng xác định mức độ nhạy cảm của thông tin liên quan hoặc những đối tượng bị ảnh hưởng bởi sự cố:.....					

.....

Ngày phát hiện sự cố (*) …/…/….. (dd/mm/yy)	Thời điểm phát hiện (*):	..... giờ.... phút

HIỆN TRẠNG SỰ CỐ (*)

- Đã được xử lý
- Chưa được xử lý

CÁCH THỨC PHÁT HIỆN * (*Đánh dấu những cách thức được sử dụng để phát hiện sự cố)*

- Qua hệ thống phát hiện xâm nhập
- Kiểm tra dữ liệu lưu lại (Log File)
- Nhận được thông báo từ: .....
- Khác, đó là.....

ĐÃ GỬI THÔNG BÁO SỰ CỐ CHO *

- Sở Thông tin và Truyền thông
- ISP đang trực tiếp cung cấp dịch vụ
- Các cơ quan chuyên trách ATTT khác

THÔNG TIN BỔ SUNG VỀ HỆ THỐNG XẢY RA SỰ CỐ

- Hệ điều hành: ..... Version: .....
- Các dịch vụ có trên hệ thống (*Đánh dấu những dịch vụ được sử dụng trên hệ thống)*
  - Web server Mail server Database server
  - Dịch vụ khác, đó là.....
- Các biện pháp ATTT đã triển khai (*Đánh dấu những biện pháp đã triển khai)*
  - Antivirus
  - Firewall
  - Hệ thống phát hiện xâm nhập
  - Khác: .....
- .....Các địa chỉ IP của hệ thống *(Liệt kê địa chỉ IP sử dụng trên Internet (IP public), không liệt kê địa chỉ IP nội bộ)*

  .....
- Các tên miền của hệ thống

.....

- Mục đích chính sử dụng hệ thống.....

.....

- Thông tin gửi kèm
  - Nhật ký hệ thống
  - Mẫu virus/mã độc
  - Khác: .....
- Các thông tin cung cấp trong thông báo sự cố này đều phải được giữ bí mật:
  - Có
  - Không

KIẾN NGHỊ, ĐỀ XUẤT HỖ TRỢ

Mô tả về đề xuất, kiến nghị
Đề nghị cung cấp tóm lược về các kiến nghị và đề xuất hỗ trợ ứng cứu (nếu có): …… …… …… ……

THỜI GIAN THỰC HIỆN BÁO CÁO SỰ CỐ *:

.../.../...../.../... (ngày/tháng/năm/giờ/phút)

Nơi nhận:
- Sở Thông tin và Truyền thông;
- Lưu: VT,....

THỦ TRƯỞNG CƠ QUAN
(Ký số)

***Chú thích**: Phần (*) là những thông tin bắt buộc, các phần còn lại có thể loại bỏ nếu không có thông tin.*

(Mẫu số 04)

TÊN CƠ QUAN CHỦ QUẢN **TÊN CƠ QUAN** Số: …../BC-	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc** *Đà Nẵng, ngày ... tháng ... năm ...*

BÁO CÁO HOÀN THÀNH XỬ LÝ SỰ CỐ AN TOÀN THÔNG TIN

THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN BÁO CÁO

▪ Tên tổ chức/cá nhân báo cáo sự cố (*) .....

▪ Địa chỉ: (*) .....

▪ Điện thoại (*)……. Email (*).....

VĂN BẢN BÁO CÁO BAN ĐẦU SỰ CỐ:

▪ Số ký hiệu …… Ngày ban hành: …/…/.....

THÔNG TIN CHI TIẾT VỀ HỆ THỐNG BỊ SỰ CỐ

Tên đơn vị vận hành HTTT (*):	*Điền tên đơn vị vận hành hoặc được thuê vận hành HTTT*				
Cơ quan chủ quản:	*Điền tên cơ quan chủ quản*				
Tên hệ thống bị sự cố	*Điền tên hệ thống bị sự cố*				
Phân loại cấp độ của HTTT, (nếu có)	☐ Cấp độ 1	☐ Cấp độ 2	☐ Cấp độ 3	☐ Cấp độ 4	☐ Cấp độ 5

Tên/Mô tả về sự cố
Đề nghị cung cấp một bản tóm tắt ngắn gọn về sự cố, bao gồm đánh giá sơ bộ cuộc tấn công đã xảy ra chưa và bất kỳ các nguy cơ dẫn đến khả năng phá hoại hoặc gián đoạn dịch vụ. Cũng vui lòng xác định mức độ nhạy cảm của thông tin liên quan hoặc những đối tượng bị ảnh hưởng bởi sự cố. (Chỉ mô tả những cập nhật mới có thay đổi so với phần mô tả của văn bản thông báo sự cố đã gửi)

Ngày phát hiện sự cố (*) (dd/mm/yy)	…/…/…..	Thời gian phát hiện (*):	…… giờ ..... phút

Kết quả xử lý sự cố
Cung cấp, tóm tắt tổng quát về những gì đã xảy ra và cách thức giải quyết, đề xuất giải pháp ứng cứu ứng sự cố nhằm xử lý nhanh sự cố, giảm nhẹ rủi ro và thiệt hại đối với sự cố tương tự trong tương lai...

Các tài liệu đính kèm
Liệt kê các tài liệu liên quan (báo cáo diễn biến sự cố; phương án xử lý, log file…..)

Nơi nhận:
- Sở Thông tin và Truyền thông;
- Lưu: VT,....

THỦ TRƯỞNG CƠ QUAN
(Ký số)

(Mẫu số 05)

TÊN CƠ QUAN CHỦ QUẢN **TÊN CƠ QUAN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: ……/BC-	*Đà Nẵng, ngày ... tháng ... năm ...*

BÁO CÁO ĐỊNH KỲ TÌNH HÌNH AN TOÀN THÔNG TIN

1. Về chính sách, quản lý

a) Đã xây dựng Quy chế bảo đảm an toàn thông tin (ATTT) nội bộ?

☐ Có (*ghi số hiệu văn bản)* ☐ Chưa

b) Đã xây dựng Kế hoạch ứng phó sự cố ATTT thông thường?

☐ Có *(ghi số hiệu văn bản)* ☐ Không

c) Có bộ phận phụ trách ATTT?

☐ Có ☐ Không

Nếu có, bộ phận có người phụ trách là:

☐ Lãnh đạo cơ quan

☐ Chuyên viên chuyên trách CNTT

☐ Khác: ……

d) Xác định cấp độ ATTT

- Các HTTT đã được phê duyệt cấp độ ATTT (*liệt kê cụ thể tên HTTT, quyết định phê duyệt cấp độ*):

- Các HTTT chưa được phê duyệt cấp độ ATTT (*liệt kê cụ thể tên HTTT chưa được phê duyệt*):

đ) Có HTTT được lưu ký ngoài Trung tâm dữ liệu thành phố?

☐ Có ☐ Không

Nếu có, báo cáo các nội dung sau:

- Tên HTTT:

- Đơn vị cung cấp dịch vụ lưu ký (*tên đơn vị, địa chỉ, số điện thoại*):

e) Có thực hiện kiểm định ATTT đối với HTTT mới được xây dựng trong năm?

☐ Có ☐ Không

Nếu có, báo cáo các nội dung sau:

- Tên HTTT:

- Đơn vị thực hiện kiểm định (*tên đơn vị, địa chỉ, số điện thoại*):

g) Có thực hiện đánh giá rủi ro ATTT trong năm?

☐ Có ☐ Không

Nếu có, báo cáo các nội dung sau:

- Tên HTTT:

- Đơn vị thực hiện đánh giá (*tên đơn vị, địa chỉ, số điện thoại*):

- Các biện pháp đã triển khai xử lý rủi ro:

h) Các công cụ bảo đảm ATTT đang thực hiện

Công cụ	Tên/phiên bản	Năm đưa vào sử dụng	Mô tả nội dung
1. Phần mềm phòng chống mã độc (antivirus)			
2. Tường lửa			
3. Công cụ mã hóa tập tin			
4. Chữ ký số			
5. Mạng riêng ảo (VPN)			
6. Quản lý Logfile trên thiết bị			
- Thiết bị 1			Nơi lưu trữ
- Thiết bị 2			Nơi lưu trữ
- Thiết bị n			Nơi lưu trữ
7. Quản lý Logfile trên máy chủ			
- Máy chủ 1			Nơi lưu trữ
- Máy chủ 2			Nơi lưu trữ
- Máy chủ n			Nơi lưu trữ
8. Các biện pháp khác:			

2. Về đầu tư

a) Kinh phí đầu tư cho công tác bảo đảm ATTT: ..... triệu đồng

b) Tỷ lệ kinh phí trên tổng kinh phí CNTT để đầu tư vào việc bảo đảm ATTT: …….%

c) Đã đầu tư vào lĩnh vực nào dưới đây:

Lĩnh vực	Mô tả nội dung	Kinh phí (đồng)
1. Mua sắm thiết bị, phần mềm chuyên dụng ATTT	(Mô tả thiết bị, phần mềm)	
2. Mua sắm hệ điều hành, phần mềm bản quyền	(Mô tả hệ điều hành, phần mềm)	
3. Tổ chức đào tạo, tập huấn, hội nghị, hội thảo về ATTT	(Mô tả nội dung, thời gian, đối tượng đào tạo, tập huấn, hội nghị, hội thảo)	
4. Xây dựng hồ sơ đề xuất cấp độ		
5. Tổ chức kiểm định HTTT mới được thiết kế		
6. Tổ chức đánh giá, xử lý rủi ro ATTT		

7. Tổ chức ứng cứu xử lý sự cố ATTT		
8. Các lĩnh vực khác:…….		

3. Về tình hình ATTT và xử lý sự cố

a) Tổng kết về các sự cố ATTTT đã xảy ra trong năm đối với cơ quan

Sự cố	Số lượng	Biện pháp xử lý
1. Tấn công chiếm quyền điều khiển		
2. Tấn công từ chối dịch vụ		
3. Tấn công mã hóa dữ liệu		
4. Tấn công phá hoại dữ liệu		
5. Tấn công thay đổi giao diện website		
6. Lừa đảo (Phishing)		
7. Thư rác (Spam mail)		
8. Lỗi hạ tầng kỹ thuật, thiết bị, phần mềm		
9. Lỗi quản trị, vận hành		
10. Sự cố khác:		

Biện pháp xử lý: Lựa chọn điền các thông tin sau (1) Không xử lý; (2) Tự xử lý; (3) Báo cáo cơ quan điều phối (Sở TT&TT); (4) Hỗ trợ từ cơ quan khác; (5) Nếu biện pháp khác thì mô tả cụ thể.

b) Mức độ thiệt hại ước tính trong năm 20... do các sự cố ATANTT gây ra

- Thiệt hại gián tiếp: ……triệu đồng
- Thiệt hại trực tiếp: …… triệu đồng
- Chi phí khắc phục: ……triệu đồng

c) Cho biết công việc mà cơ quan đã thực hiện sau khi khắc phục được sự cố trong năm qua

- Liên kết, để được hỗ trợ từ các đơn vị hoạt động trong lĩnh vực ATTT
- Sửa đổi chính sách/hướng dẫn/thủ tục
- Nâng cao ý thức;
- Tăng cường thiết bị
- Rà soát lại hệ thống;
- Công việc khác (*mô tả cụ thể*):

……..

……..

……..

……..

4. Kiến nghị, đề xuất

……..

……..
……..
……..

Người lập báo cáo:
- Họ và tên:
- Chức vụ:
- Điện thoại:
- Email:

THỦ TRƯỞNG CƠ QUAN
(Ký số)

***Ghi chú**:*

- Điền thông tin đầy đủ vào các câu hỏi: Để lựa chọn đánh dấu X

- Câu hỏi với ký hiệu ❗ trước mối lựa chọn thì chỉ được phép đánh dấu một kết quả (chọn một)

- Câu hỏi với ký hiệu ▬ trước mỗi lựa chọn thì có thể đánh dấu từ không tới nhiều kết quả (chọn nhiều)

- Ký số và gửi liên thông về Sở Thông tin và Truyền thông.