UBND TỈNH BẮC NINH **THANH TRA TỈNH**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 143 /QĐ-TTr	*Bắc Ninh, ngày 08 tháng 12 năm 2023*

QUYẾT ĐỊNH
V/v ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Thanh tra tỉnh Bắc Ninh

CHÁNH THANH TRA TỈNH BẮC NINH

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 Luật An ninh mạng ngày 12/06/2018;

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 15/7/2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12/09/2017 của 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 27/2017/TT-BTTTT ngày 20/10/2017 của Bộ Thông tin và Truyền thông quy định về quản lý, vận hành, kết nối, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;

Căn cứ Quyết định số 21/2019/QĐ-UBND ngày 22/10/2019 của UBND tỉnh về việc ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước trên địa bàn tỉnh Bắc Ninh;

Căn cứ Quyết định số 483/2014/QĐ-UBND ngày 20/11/2014 của UBND tỉnh Bắc Ninh về việc ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Thanh tra tỉnh Bắc Ninh.

Xét đề nghị của Chánh Văn phòng Thanh tra tỉnh,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Thanh tra tỉnh Bắc Ninh".

Điều 2. Quyết định có hiệu lực thi hành kể từ ngày ký ban hành và thay thế Quyết định số 157/QĐ-TTr ngày 29/12/2017 của Thanh tra tỉnh Bắc Ninh.

Các ông: Chánh Văn phòng, Trưởng các phòng Nghiệp vụ thuộc Thanh tra tỉnh và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Sở Thông tin và Truyền thông;
- Lãnh đạo Thanh tra tỉnh;
- Cổng TTĐT Thanh tra tỉnh (đ/c Quang, P.TP NV4 để đăng tải);
- Lưu: VT, CVP, TH.

CHÁNH THANH TRA

Trần Quang Ứng

UBND TỈNH BẮC NINH
THANH TRA TỈNH

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Bắc Ninh, ngày tháng năm 2023

QUY CHẾ
Bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Thanh tra tỉnh Bắc Ninh

(Ban hành kèm theo Quyết định số /QĐ-TTr ngày / /2023 của Thanh tra tỉnh Bắc Ninh)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi áp dụng

Quy chế này quy định về việc bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Thanh tra tỉnh Bắc Ninh.

2. Đối tượng áp dụng

Quy chế này áp dụng đối với Văn phòng, các phòng Nghiệp vụ thuộc Thanh tra tỉnh Bắc Ninh (sau đây gọi tắt là Thanh tra tỉnh); các Đoàn thanh tra, Đoàn (Tổ) xác minh giải quyết đơn; các cá nhân là công chức, người lao động liên quan đến hoạt động ứng dụng công nghệ thông tin của Thanh tra tỉnh.

Điều 2. Mục đích, nguyên tắc bảo đảm an toàn thông tin mạng

1. Việc áp dụng Quy chế này nhằm phòng ngừa, ngăn chặn, xử lý và giảm các nguy cơ gây mất an toàn thông tin mạng và bảo đảm an ninh thông tin trong quá trình ứng dụng công nghệ thông tin trong hoạt động của Thanh tra tỉnh.

2. Hoạt động ứng dụng công nghệ thông tin của Thanh tra tỉnh phải tuân thủ theo nguyên tắc bảo đảm an toàn thông tin mạng được quy định tại Điều 4 Luật An toàn thông tin mạng số 86/2015/QH15 ngày 19/11/2015 và Điều 41 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.

Điều 3. Giải thích từ ngữ

1. *Mạng:* là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính.

2. *Hệ thống mạng*: bao gồm dịch vụ kết nối Internet; mạng nội bộ; mạng truyền số liệu chuyên dùng

3. *Mạng nội bộ (LAN):* là tập hợp các trang thiết bị công nghệ thông tin được kết nối với nhau thông qua các bộ chuyển mạch, bộ định tuyến, bộ điểm truy cập và các máy chủ, thiết bị quản lý mạng, phần mềm quản lý mạng, thiết bị an toàn hệ thống mạng trong phạm vi quản lý của Thanh tra tỉnh. Mạng nội bộ

bao gồm mạng nội bộ có dây và mạng nội bộ không dây (Wifi).

4. *Đơn vị vận hành hệ thống thông tin:* là đơn vị chủ trì việc quản lý và vận hành kỹ thuật hệ thống thông tin.

5. *An toàn thông tin mạng:* được quy định tại Khoản 1 Điều 3 Luật An toàn thông tin mạng. Cụ thể: An toàn thông tin mạng là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

6. *Hệ thống thông tin:* được quy định tại khoản 3 Điều 3 Luật An toàn thông tin mạng. Cụ thể: Hệ thống thông tin là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng.

7. *Xâm phạm an toàn thông tin mạng:* được quy định tại khoản 6 Điều 3 Luật An toàn thông tin mạng. Cụ thể: Xâm phạm an toàn thông tin mạng là hành vi truy nhập, sử dụng, tiết lộ, làm gián đoạn, sửa đổi, phá hoại trái phép thông tin, hệ thống thông tin.

8. *Sự cố an toàn thông tin mạng:* được quy định tại khoản 7 Điều 3 Luật An toàn thông tin mạng. Cụ thể: Sự cố an toàn thông tin mạng là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

9. *Rủi ro an toàn thông tin mạng:* được quy định tại khoản 8 Điều 3 Luật An toàn thông tin mạng. Cụ thể: Rủi ro an toàn thông tin mạng là những nhân tố chủ quan hoặc khách quan có khả năng ảnh hưởng tới trạng thái an toàn thông tin mạng.

10. *Phần mềm độc hại:* được quy định tại khoản 11 Điều 3 Luật An toàn thông tin mạng. Cụ thể: Phần mềm độc hại là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

Điều 4. Các hành vi bị nghiêm cấm

1. Các hành vi bị nghiêm cấm về an toàn, an ninh thông tin mạng quy định tại Điều 7 Luật An toàn thông tin mạng và Điều 8 Luật An ninh mạng.

2. Tự ý lắp đặt các thiết bị phát sóng Wifi (Access Point) vào mạng máy tính của cơ quan và lắp đặt các thiết bị tiếp sóng Wifi (Wireless card, wireless USB) trên máy tính có kết nối mạng nội bộ để truy cập mạng wifi ngoài khi chưa được phê duyệt của Lãnh đạo cơ quan.

3. Lợi dụng mạng để truyền bá thông tin, quan điểm, thực hiện các hành vi gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, lợi ích quốc gia trên mạng; phá hại khối đại đoàn kết toàn dân; tuyên truyền chiến tranh xâm lược, khủng bố; gây hận thù, mâu thuẫn giữa các dân tộc, sắc tộc, tôn giáo.

4. Lợi dụng mạng để truyền bá trái phép tài liệu, hình ảnh, âm thanh hoặc dạng thông tin khác nhằm 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; bôi nhọ, gây thù hận, xâm hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân.

5. Tự ý đăng lên, tải về, chia sẻ dưới mọi hình thức các dữ liệu, tài liệu, số liệu nội bộ, những văn bản chưa được cấp có thẩm quyền công khai lên mạng internet và các phương tiện thông tin đại chúng khác.

Điều 5. Phân công bộ phận chuyên trách và công tác phối hợp với những cơ quan/tổ chức có thẩm quyền về an toàn thông tin mạng

1. Phân công bộ phận chuyên trách về an toàn thông tin mạng:

Giao Văn phòng Thanh tra tỉnh là bộ phận chuyên trách về an toàn thông tin mạng.

2. Nhiệm vụ của bộ phận chuyên trách về an toàn thông tin mạng:

a) Là đầu mối liên hệ, tiếp nhận, phối hợp với các cơ quan, tổ chức (có thẩm quyền quản lý về an toàn thông tin mạng) trong công tác đảm bảo an toàn thông tin mạng, hỗ trợ điều phối xử lý sự cố an toàn thông tin mạng.

b) Là đầu mối liên hệ, phối hợp với Sở Thông tin và Truyền thông và các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin mạng, phục vụ việc bảo đảm an toàn, an ninh mạng cho các hệ thống triển khai tại Thanh tra tỉnh.

c) Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của cơ quan, tổ chức có thẩm quyền.

d) Làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trong nội bộ cơ quan Thanh tra tỉnh.

đ) 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 an toàn thông tin mạng kịp thời, nhanh chóng và đạt hiệu quả.

e) Phối hợp chặt chẽ với Công an tỉnh, Sở Thông tin và Truyền thông và các đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin mạng.

f) Định kỳ hằng năm lập báo cáo về tình hình an toàn thông tin mạng, gửi về Sở Thông tin và Truyền thông (theo hướng dẫn của Sở Thông tin và Truyền thông).

Điều 6. Bảo đảm nguồn nhân lực

1. Xây dựng Đề án vị trí việc làm, có vị trí về công nghệ thông tin. Khi tuyển dụng, tiếp nhận cán bộ chuyên trách vào vị trí việc làm về an toàn thông tin/công nghệ thông tin phải có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí việc làm. Cán bộ chuyên trách hoặc cán bộ kiêm nhiệm được đảm bảo các điều kiện học tập, tiếp cận công nghệ, kiến thức an toàn bảo mật thông tin trước khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ.

2. Cán bộ được giao nhiệm vụ quản lý, vận hành truy cập, khai thác đối với các hệ thống thông tin, thực hiện theo trách nhiệm và phân quyền; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài; theo dõi và phát hiện các trường hợp truy cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, báo cáo cho cán bộ quản lý để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm.

3. Thường xuyên tổ chức, phổ biến các quy định về đảm bảo an toàn thông tin, nhằm nâng cao nhận thức về trách nhiệm đảm bảo an toàn thông tin cho các phòng Nghiệp vụ, cá nhân sử dụng hệ thống thông tin do đơn vị quản lý.

4. Có kế hoạch và định kỳ hàng năm tổ chức đào tạo về an toàn thông tin hàng năm cho 03 nhóm đối tượng bao gồm: Cán bộ kỹ thuật, cán bộ quản lý và người sử dụng hệ thống.

5. Cán bộ được giao nhiệm vụ quản lý, vận hành truy cập khi nghỉ hưu hoặc thay đổi công việc khác, phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của Thanh tra tỉnh; thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống và có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ hưu hoặc thay đổi công việc khác.

Chương II:
BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ VẬN HÀNH HỆ THỐNG THÔNG TIN

Điều 7. Quản lý an toàn mạng

1. Hệ thống mạng được tổ chức quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý hệ thống chặt chẽ, bảo đảm an toàn và bảo mật.

2. Hệ thống mạng nội bộ (LAN) phải được bảo vệ bằng tường lửa (có thể tích hợp tường lửa trên modem hoặc router) và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng (nếu có).

3. Mạng không dây (WIFI), cần thiết lập các thông số an toàn và định kỳ ít nhất 3 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật. Hệ thống mạng không dây phải được bảo vệ bởi mật khẩu an toàn.

4. Quản lý, vận hành hoạt động bình thường của hệ thống:

a) Thường xuyên kiểm tra cấu hình, các file nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện và xử lý những sự cố nếu có.

b) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm.

c) Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp.

d) Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng.

e) Các bản quyền phần mềm cần được thống kê, quản lý thời gian phục vụ cho việc gia hạn.

5. Truy cập và quản lý cấu hình hệ thống:

a) Cán bộ quản lý, nhân viên vận hành truy cập, khai thác thông tin tại hệ thống theo trách nhiệm và phân quyền; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài.

b) Cán bộ quản lý, nhân viên vận hành có trách nhiệm theo dõi và phát hiện các trường hợp truy cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, báo cáo cho cán bộ quản lý để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm.

c) Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác.

d) Quy trình kết nối thiết bị đầu cuối của người sử dụng vào hệ thống mạng; truy nhập và quản lý cấu hình hệ thống; cấu hình tối ưu, tăng cường bảo mật cho thiết bị mạng, bảo mật (cứng hóa) trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác.

6. Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác.

7. Việc thanh lý, tiêu hủy thiết bị, vật mang thông tin trong mạng phải đảm bảo yêu cầu không để lộ, lọt thông tin Nhà nước. Phải có quy trình cụ thể và phải lưu giữ hồ sơ, biên bản việc thanh lý, tiêu hủy.

Điều 8. Quản lý phòng chống phần mềm độc hại

1. Tất cả các máy trạm phải được trang bị phần mềm phòng chống mã độc. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin.

2. Khi gửi văn bản điện tử gửi qua hệ thống thư điện tử phải có định dạng theo Danh mục tiêu chuẩn kỹ thuật về ứng dụng CNTT trong cơ quan nhà nước như: (.txt), (.doc), (.odt), (.pdf) và các định dạng khác theo quy định, không được gửi các file thực thi (.com),(.bat),(.exe)....

3. Các công 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.

4. Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu,…), người sử dụng phải báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý.

5. Phần mềm ứng dụng trước khi được cài đặt, sử dụng phải được kiểm tra xem có phần mềm độc hại tồn tại hay không. Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng.

7. Định kỳ hàng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; Thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống.

Điều 9. Quản lý giám sát an toàn hệ thống thông tin

1. Triển khai hệ thống giám sát trung tâm phải đáp ứng yêu cầu tại khoản 1, Điều 5 Thông tư số 31/2017/TT-BTTTT.

2. Thông tin giám sát và danh mục các đối tượng giám sát phải đáp ứng yêu cầu tại khoản 2, Điều 5 Thông tư số 31/2017/TT-BTTTT; Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát.

3. Thực thi nhiệm vụ giám sát theo quy định tại khoản 3, Điều 5 Thông tư số 31/2017/TT-BTTTT.

4. Định kỳ hàng năm tổ chức nâng cao năng lực hoạt động giám sát theo quy định tại Điều 9 Thông tư số 31/2017/TT-BTTTT.

5. Chủ quản hệ thống thông tin có trách nhiệm giám sát an toàn thông tin theo quy định tại Điều 14 Thông tư số 31/2017/TT-BTTTT.

Điều 10. Quản lý điểm yếu an toàn hệ thống thông tin

1. Bộ phận chuyên trách về an toàn thông tin có trách nhiệm:

a) Quản lý thông tin điểm yếu an toàn thông tin đối với từng thành phần có trong hệ thống (hệ điều hành, máy chủ, ứng dụng, dịch vụ…); Phân loại mức độ nguy hiểm của điểm yếu; Xây dựng phương án xử lý đối với từng mức độ nguy hiểm của điểm yếu.

b) Báo cáo Lãnh đạo/Cán bộ quản lý ngay khi phát hiện điểm yếu an toàn thông tin ở mức độ nghiêm trọng. Thực hiện cảnh báo và xử lý điểm yếu an toàn thông tin theo chỉ đạo. Việc xử lý điểm yếu an toàn thông tin phải bảo đảm không giám ảnh hưởng/gián đoạn hoạt động của hệ thống.

c) Xây dựng phương án xử lý tạm thời đối với trường hợp điểm yếu an toàn thông tin chưa được khắc phục và phương án khôi phục hệ thống trong trường hợp xử lý điểm yếu thất bại.

đ) Có trách nhiệm phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin đối với các điểm yếu khi cần thiết.

2. Đối với hệ thống/hệ thống thành phần được đề xuất là cấp độ 3 trở lên phải thực hiện kiểm tra, đánh giá và xử lý điểm yếu an toàn thông tin cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng.

3. Định kỳ hàng năm kiểm tra, đánh giá điểm yếu an toàn thông tin cho toàn bộ hệ thống thông tin; Thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin khi có thông tin hoặc nhận được cảnh báo về điểm yếu an toàn thông tin đối với thành phần cụ thể trong hệ thống.

4. Hoạt động đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thực hiện theo quy định tại điểm c khoản 2 Điều 20 Nghị định số 85/2016/NĐ-CP và Điều 13 Thông tư số 03/2017/TT-BTTTT.

Điều 11. Quản lý an toàn dữ liệu

1. Yêu cầu an toàn đối với phương pháp mã hóa

a) Xây dựng và áp dụng quy định sử dụng các phương thức mã hóa thích hợp theo các chuẩn quốc gia hoặc quốc tế đã được công nhận để bảo vệ thông tin.

b) Có biện pháp quản lý khóa mã hóa thích hợp để hỗ trợ việc sử dụng các kỹ thuật mã hóa.

2. Phân loại, quản lý và sử dụng khóa bí mật và dữ liệu mã hóa.

3. Cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu.

4. Sao lưu dự phòng và khôi phục dữ liệu (tần suất sao lưu dự phòng, phương tiện lưu trữ, thời gian lưu trữ; nơi lưu trữ, phương thức lưu trữ và phương thức lấy dữ liệu ra khỏi phương tiện lưu trữ).

5. Trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ.

6. Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ.

7. Có cơ chế sao lưu dữ liệu dự phòng, lưu trữ dữ liệu tại nơi an toàn đồng thời thường xuyên kiểm tra để đảm bảo sẵn sàng phục hồi nhằm ngăn ngừa và hạn chế khi sự cố an toàn thông tin mạng xảy ra. Dữ liệu trên máy chủ được sao lưu thông qua hệ thống sao lưu dữ liệu.

8. Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: Tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ và các thông tin, dữ liệu quan trọng khác trên hệ thống theo yêu cầu của đơn vị vận hành.

9. Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của nhân viên và phải được phê duyệt từ cấp trên.

10. Thực hiện quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn.

11. Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ/phương tiện lưu trữ.

Điều 12. Quản lý an toàn người sử dụng đầu cuối

1. Việc sử dụng các thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB,... phải thường xuyên quét virus trước khi đọc hoặc sao chép dữ liệu.

2. Không sử dụng các máy tính thuộc sở hữu cá nhân (máy xách tay của cá nhân, PDA) vào mục đích cơ quan hoặc những thiết bị lưu trữ di động của cá

nhân vào mục đích của cơ quan. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu.

3. Các thiết bị đầu cuối khi kết nối phải được quản lý và cập nhật thông tin (tên, chủng loại, địa chỉ MAC, địa chỉ IP). Cần sử dụng cơ chế xác thực và sử dụng giao thức mạng an toàn.

4. Bộ phận chuyên trách về an toàn thông tin phải thường xuyên theo dõi, kiểm tra các lỗ hổng bảo mật và quản lý kết nối, truy cập khi sử dụng thiết bị đầu cuối từ xa.

5. Bộ phận chuyên trách về an toàn thông tin thường xuyên theo dõi cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống đối với các nhân viên đã nghỉ việc.

6. Bộ phận chuyên trách về an toàn thông tin thường xuyên theo dõi cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho máy tính người sử dụng và thực hiện quy trình trước khi đưa hệ thống vào sử dụng.

7. Quản lý truy cập, sử dụng tài nguyên nội bộ

a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin và các quy định của cơ quan, tổ chức.

b) Khi cài đặt, kết nối máy tính/thiết bị đầu cuối phải thực hiện theo hướng dẫn/quy trình dưới sự giám sát của bộ phận chuyên trách về an toàn thông tin.

c) Máy tính/thiết bị đầu cuối phải được xử lý điểm yếu an toàn thông tin, cấu hình cứng hóa bảo mật trýớc khi kết nối vào hệ thống.

d) Đối với hệ thống thông tin có cấp độ 3 trở lên, máy tính/thiết bị đầu cuối phải được xử lý điểm yếu an toàn thông tin, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống.

8. Quản lý truy cập mạng và tài nguyên trên Internet:

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 mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao.

b) 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 mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý.

d) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được tỉnh hoặc đơn vị chuyên môn tổ chức.

9. Cài đặt và sử dụng máy tính an toàn.

Điều 13. Quản lý sự cố an toàn thông tin

1. Phân nhóm sự cố an toàn thông tin, 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, đơn vị như: máy tính trạm bị nhiễm phần mềm độc hại, phần mềm hệ điều hành, các phần mềm ứng dụng cài đặt trên máy tính cá nhân phát sinh lỗi.

b) Trung bình: Sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của đơn vị như: hệ thống mạng của 01 (một) phòng Nghiệp vụ, Văn phòng bị ngưng hoạt động, phần mềm độc hại lây nhiễm tất cả các máy tính trạm trong phòng Nghiệp vụ, Văn phòng.

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 như: hệ thống quản lý văn bản và điều hành, văn bản, tài liệu điện tử của đơn vị bị ngưng hoạt động, một số thiết bị công nghệ thông tin quan trọng (bộ chuyển mạch trung tâm, thiết bị định tuyến, thiết bị tường lửa, máy chủ quản lý tập tin chung,) bị hư hỏng.

d) Khẩn cấp: Sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của cơ quan, đơn vị như: toàn bộ hệ thống thiết bị công nghệ thông tin, hệ thống cung cấp điện ngừng hoạt động, hệ thống trang thông tin điện tử bị tin tặc (hacker) tấn công, xâm nhập, thay đổi nội dung...

2. Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin:

Khi có sự cố hoặc nguy cơ mất an toàn thông tin mạng xảy ra như: Hệ thống hoạt động chậm bất thường, không truy cập được hệ thống, nội dung thông tin bị thay đổi không chủ động hoặc các dấu hiệu bất thường khác thì tiến hành quy trình ứng cứu sự cố theo các bước sau:

a) Bước 1: Nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc thẩm quyền cơ quan, đơn vị trực tiếp quản lý thì thực hiện tiếp Bước 2. Nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc Trung tâm Công nghệ thông tin và Truyền thông trực thuộc Sở Thông tin và Truyền thông quản lý (các hệ thống được triển khai tập trung tại Trung tâm Dữ liệu tỉnh) thì thực hiện tiếp Bước 3.

b) Bước 2: Tiến hành xử lý sự cố theo quy chế nội bộ của cơ quan, đơn vị. Nếu sự cố được khắc phục thì lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố. Khi sự cố vượt quá khả năng xử lý của cơ quan, lập biên bản ghi nhận và thực hiện tiếp Bước 3.

c) Bước 3: Báo sự cố đến Sở Thông tin và Truyền thông theo mẫu tại Phụ lục 1 kèm Quy chế và thực hiện tiếp Bước 4.

d) Bước 4: Phối hợp với Trung tâm Công nghệ thông tin và Truyền thông trực thuộc Sở Thông tin và Truyền thông và các cơ quan, tổ chức có liên quan để tiến hành khắc phục sự cố và thực hiện tiếp Bước 5.

đ) Bước 5: Lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố theo mẫu tại Phụ lục 2 kèm Quy chế, lãnh đạo cơ quan, đơn vị phải chỉ đạo kịp thời để khắc phục và hạn chế thiệt hại, báo cáo bằng văn bản cho cơ quan cấp trên trực tiếp quản lý và Sở Thông tin và Truyền thông.

Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của cơ quan, lãnh đạo cơ quan phải báo cáo ngay cho Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ.

3. Bộ phận chuyên trách về an toàn thông tin có trách nhiệm

a) Phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia (Quyết định số 05/2017/QĐ-TTg); Xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng, ứng phó sự cố an toàn thông tin mạng.

b) Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13, 14 Quyết định số 05/2017/QĐ-TTg.

c) Phối hợp với các đơn vị chức năng xây dựng và triển khai kế hoạch ứng phó sự cố an toàn thông tin theo quy định tại Điều 16 Quyết định số 05/2017/QĐ-TTg.

d) Có phương án và điều động nhân lực có kinh nghiệm thực hiện giám sát, phát hiện và cảnh báo sự cố an toàn thông tin, phối hợp với các đơn vị chuyên trách về ATTT đưa ra cảnh bảo sớm về nguy cơ mất ATTT trong hệ thống.

e) Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13, 14 Quyết định số 05/2017/QĐ-TTg.

f) Phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin; Yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống.

g) Quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về ATTT; Hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; Yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; Phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo.

h) Phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin; Yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống.

4. Trách nhiệm của người dùng

Thông tin, báo cáo kịp thời cho cán bộ chuyên trách về ATTT của cơ quan khi phát hiện các sự cố gây mất ATTT trong quá trình tham gia vào hệ thống thông tin của đơn vị; Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

Điều 14. Quản lý an toàn thông tin của cơ quan, đơn vị đối với người sử dụng

1. Khi tiếp nhận nhân sự mới phải có trách nhiệm phổ biến cho nhân sự mới các quy định về bảo đảm an toàn thông tin mạng tại cơ quan, đơn vị.

2. Phải thường xuyên tổ chức quán triệt các quy định về an toàn thông tin mạng, nhằm nâng cao nhận thức về trách nhiệm bảo đảm an toàn thông tin mạng của từng cá nhân trong cơ quan, đơn vị.

3. Đối với cán bộ chấm dứt hoặc thay đổi công việc thực hiện theo điểm a, khoản 3, Điều 6 tại Quy định này.

Điều 15. Quản lý truy cập

1. Đối với Văn phòng, các phòng Nghiệp vụ và người sử dụng có trách nhiệm

a) Bảo vệ bí mật thông tin tài khoản cá nhân, hoặc tài khoản của cơ quan, đơn vị khi được phân công nắm giữ đồng thời phải thay đổi ngay mật khẩu tài khoản khi mới được cấp và tự chịu trách nhiệm trong việc quản lý, bảo vệ mật khẩu của tài khoản, không được cho người khác sử dụng tài khoản cá nhân hoặc của cơ quan, đơn vị.

b) Không đặt chế độ tự động ghi nhớ mật khẩu của các trình duyệt trong mọi trường hợp sử dụng.

c) Thiết lập mật mã truy cập và chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng cho tất cả hệ thống máy chủ, máy trạm của người sử dụng.

d) Hệ thống mạng không dây (wifi) của các cơ quan, đơn vị phải được đặt mật khẩu (password) khi truy cập. Thiết lập phương pháp hạn chế người dùng truy cập mạng không dây, giám sát và điều khiển truy cập mạng không dây.

đ) Đặt mật khẩu đăng nhập, truy cập hệ thống thông tin có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặc biệt như !, @, #, $, %) và phải được thay đổi ít nhất 03 tháng/lần cho tất cả các tài khoản truy cập vào hệ thống máy chủ, thiết bị mạng, máy tính, các ứng dụng.

e) Các đơn vị cần rà soát tối thiểu 03 tháng/lần các tài khoản đăng nhập, bảo đảm các tài khoản và quyền truy cập hệ thống được cấp phát đúng, đủ.

2. Đối với các hệ thống thông tin

a) Bảo đảm mỗi tài khoản của tổ chức, cá nhân truy cập vào hệ thống thông tin là duy nhất;

b) Các hệ thống thông tin cần giới hạn số lần đăng nhập sai liên tiếp vào hệ thống (từ 03 đến 05 lần). Hệ thống tự động khóa tài khoản trong một khoảng thời gian nhất định nếu liên tục đăng nhập sai vượt quá số lần quy định trước khi tiếp tục cho đăng nhập và có phương thức hỗ trợ cấp lại mật khẩu tài khoản;

c) Đơn vị quản lý, vận hành các hệ thống dùng chung sẽ không chịu trách nhiệm về những thiệt hại do phía người dùng không tuân thủ các quy định về bảo vệ bí mật tài khoản dẫn đến thông tin cá nhân bị đánh cắp hay bị sửa đổi, các ứng dụng bị sử dụng mạo danh hay các hậu quả tiêu cực khác.

Điều 16. Quản lý rủi ro an toàn thông tin

1. Xác định mức rủi ro.

2. Quy trình đánh giá và quản lý rủi ro.

3. Biện pháp kiểm soát rủi ro.

Điều 17. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

1. Quy định về bảo đảm an toàn thông tin khi kết thúc vận hành, khai thác, thanh lý, hủy bỏ.

2. Quy trình xử lý thông tin trên hệ thống khi thay đổi mục đích sử dụng hoặc gỡ bỏ.

3. Phương án kỹ thuật thực hiện xử lý thông tin trên hệ thống khi thay đổi mục đích sử dụng hoặc gỡ bỏ.

Điều 18. Bảo đảm an toàn trong xây dựng hệ thống thông tin

1. Các hoạt động liên quan đến xây dựng, thiết lập, quản lý, vận hành, nâng cấp mở rộng hệ thống thông tin phải thực hiện xác định cấp độ và phương án bảo đảm an toàn thông tin mạng 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 thông tin theo cấp độ và hướng dẫn tại Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

2. Nhiệm vụ quản lý về hướng dẫn xác định hệ thống thông tin và cấp độ an toàn hệ thống thông tin; thực hiện các yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ; thực hiện kiểm tra, đánh giá an toàn thông tin mạng; tiếp nhận và thẩm định hồ sơ đề xuất cấp độ; báo cáo, chia sẻ thông tin thực hiện theo hướng dẫn của Bộ Thông tin và Truyền thông tại Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017;

3. Bộ phận chuyên trách thực hiện việc tham mưu phối hợp với Sở Thông tin và Truyền thông và các cơ quan, đơn vị có thẩm quyền về an toàn thông tin tổ chức kiểm tra, đánh giá an toàn thông tin đối với các hệ thống thông tin; kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin.

Điều 19. Sao lưu dữ liệu dự phòng

1. Đối với Văn phòng, các phòng Nghiệp vụ và người sử dụng:

a) Khi lưu trữ, khai thác, trao đổi thông tin, dữ liệu phải bảo đảm tính toàn vẹn, tính tin cậy, tính sẵn sàng. Khi lưu trữ, trao đổi thông tin, dữ liệu quan trọng phải áp dụng kỹ thuật mã hóa, thiết lập mật mã, ứng dụng chữ ký số và phải có cơ chế lưu trữ dự phòng;

b) Phải lập kế hoạch và thực hiện sao lưu dữ liệu dự phòng định kỳ ít nhất một lần trong tháng các dữ liệu quan trọng được triển khai, lưu trữ (bao gồm dữ liệu phát sinh trong quá trình vận hành các phần mềm ứng dụng như: các tập tin văn bản, hình ảnh, các tập tin dữ liệu khác). Sau khi sao lưu, lưu trữ bản sao lưu bằng thiết bị lưu trữ ngoài (như: đĩa quang, ổ cứng ngoài, các thiết bị lưu trữ khác) theo quy định lưu trữ hiện hành, bảo đảm tính sẵn sàng, bảo mật và toàn vẹn nhằm đáp ứng yêu cầu phục hồi dữ liệu, khắc phục hệ thống thông tin cho hoạt động bình thường kịp thời khi có sự cố xảy ra.

2. Đối với đơn vị chủ quản các hệ thống thông tin

a) Có trách nhiệm ban hành và thực hiện quy trình sao lưu dự phòng và phục hồi cho các phần mềm, dữ liệu;

b) Xây dựng 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) Phải lưu trữ dữ liệu sao lưu ở nơi an toàn, không cùng phân vùng lưu trữ các ứng dụng và được kiểm tra thường xuyên, bảo đảm sẵn sàng cho việc sử dụng khi cần thiết.

Chương III
BÁO CÁO, CHIA SẺ THÔNG TIN

Điều 20. Chế độ báo cáo

1. Báo cáo định kỳ

Báo cáo an toàn thông tin định kỳ hàng năm gồm các nội dung quy định tại khoản 3 Điều 17 Thông tư 03/2017/TT-BTTTT gửi Sở Thông tin và Truyền thông trước ngày 15 tháng 11 hàng năm.

2. Báo cáo đột xuất

Báo cáo về công tác khắc phục mã độc, lỗ hổng, điểm yếu, triển khai cảnh báo an toàn thông tin và các báo cáo đột xuất khác theo yêu cầu của các cơ quan quản lý nhà nước về an toàn thông tin.

Chương IV
TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 21. Trách nhiệm của Lãnh đạo Thanh tra tỉnh Bắc Ninh

1. Thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo quy định tại quy chế này và các nhiệm vụ do chủ quản hệ thống thông tin (UBND tỉnh) phân công.

2. Chánh Thanh tra tỉnh có trách nhiệm chỉ đạo, tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước UBND tỉnh trong công tác bảo đảm an toàn thông tin mạng của cơ quan Thanh tra tỉnh.

3. Phân công bộ phận hoặc cán bộ bảo đảm an toàn thông tin mạng của đơn vị; tạo điều kiện để các cán bộ phụ trách an toàn thông tin mạng được học tập, nâng cao trình độ về an toàn thông tin mạng; thường xuyên tổ chức quán triệt các quy định về an toàn thông tin mạng trong cơ quan, đơn vị; xác định các yêu cầu, trách nhiệm bảo đảm an toàn thông tin mạng đối với các vị trí cần tuyển dụng hoặc phân công.

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 an toàn thông tin mạng kịp thời, nhanh chóng và đạt hiệu quả.

5. Phối hợp chặt chẽ với Công an tỉnh, Sở Thông tin và Truyền thông và các đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin mạng.

6. Chỉ đạo định kỳ hằng năm lập báo cáo về tình hình an toàn thông tin mạng, gửi về Sở Thông tin và Truyền thông (theo hướng dẫn của Sở Thông tin và Truyền thông).

Điều 22. Trách nhiệm đảm bảo an toàn thông tin mạng

1. Trách nhiệm của cán bộ, công chức, phụ trách quản lý vận hành hệ thống và an toàn thông tin mạng Thanh tra tỉnh:

a) Chịu trách nhiệm bảo đảm an toàn thông tin mạng của đơn vị.

b) Tham mưu lãnh đạo cơ quan, đơn vị ban hành các quy định, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin mạng.

c) Thực hiện việc giám sát, đánh giá, báo cáo thủ trưởng cơ quan, đơn vị các rủi ro mất an toàn thông tin mạng và mức độ nghiêm trọng của các rủi ro đó.

d) Phối hợp với các tổ chức, cá nhân có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn, an ninh thông tin.

đ) Phải thiết lập phương pháp hạn chế truy cập mạng không dây, giám sát và điều khiển truy cập không dây, tổ chức sử dụng chứng thực và mã hóa để bảo vệ truy cập không dây tới hệ thống thông tin.

e) Phải tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin.

2. Trách nhiệm của công chức và người lao động thuộc Thanh tra tỉnh:

a) Nghiêm túc chấp hành các quy định tại quy chế này và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao.

b) Khi tham gia vận hành mạng máy tính của cơ quan, đơn vị phải nghiêm chỉnh chấp hành chế độ bảo mật, an ninh, an toàn thông tin đồng thời chịu trách nhiệm đối với các thông tin mà mình cung cấp. Mỗi cán bộ, công chức và người lao động phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp các thiết bị trên máy tính; không được vào các trang thông tin điện tử không rõ về nội dung; không tải và cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn; không nhấp chuột vào các đường dẫn lạ không rõ về nội dung; không cho phép bất cứ hành vi nào gây tổn hại đến dịch vụ, gây hư hỏng thiết bị mạng; không cung cấp thông tin không trung thực để công bố trên mạng; sử dụng mạng để thâm nhập vào các mạng máy tính khi chưa được phép; không đưa các thông tin có nội dung "mật", "tối mật" và "tuyệt mật" lên hệ thông máy tính có kết nối mạng Internet.

c) Trong trao đổi thông tin, dữ liệu phục vụ công việc, các cơ quan, đơn vị, cán bộ, công chức, viên chức phải sử dụng hệ thống thông tin do cơ quan, đơn vị có thẩm quyền triển khai như: Hệ thông thư điện tử tỉnh (@bacninh.gov.vn) hoặc hệ thống thư điện tử của Bộ, ngành, lĩnh vực; hệ thống quản lý văn bản và điều hành. Mỗi cán bộ, công chức và người lao động không sử dụng các trang mạng xã hội, các dịch vụ thư điện tử công cộng,... để trao đổi thông tin quan trọng liên quan đến công việc chuyên môn của cơ quan, đơn vị.

d) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng 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.

đ) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng do các cơ quan, đơn vị chuyên trách về an toàn thông tin mạng hoặc Sở Thông tin và Truyền thông tổ chức.

Chương V
KHEN THƯỞNG, KỶ LUẬT

Điều 23. Khen thưởng

Các phòng Ngiệp vụ, Văn phòng thuộc Thanh tra tỉnh; công chức, người lao động cơ quan Thanh tra tỉnh thực hiện tốt quy chế này, đem lại hiệu quả thiết thực sẽ được xem xét đánh giá khen thưởng.

Điều 24. Xử lý vi phạm

Các phòng Ngiệp vụ, Văn phòng thuộc Thanh tra tỉnh; công chức, người lao động trong cơ quan vi phạm Quy chế này tùy theo tính chất, mức độ vi phạm sẽ bị xử lý kỷ luật, xử phạt hành chính, bồi thường thiệt hại hoặc bị truy cứu trách nhiệm hình sự theo quy định hiện hành.

Chương VI
TỔ CHỨC THỰC HIỆN

Điều 25. Phân công nhiệm vụ

1. Văn phòng Thanh tra tỉnh

- Tham mưu giúp Lãnh đạo Thanh tra tỉnh về công tác bảo đảm an toàn thông tin mạng Thanh tra tỉnh và chịu trách nhiệm trước Lãnh đạo Thanh tra tỉnh trong việc bảo đảm an toàn thông tin mạng cho các hệ thống thông tin của Thanh tra tỉnh;

- Thực hiện thủ tục xác định cấp độ an toàn thông tin mạng và bảo đảm an toàn cho các hệ thống thông tin theo quy định của Luật An toàn thông tin mạng, 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 và hướng dẫn tại Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

- Hàng năm xây dựng kế hoạch, tổng hợp nhu cầu của các cơ quan, đơn vị để triển khai công tác an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Thanh tra tỉnh theo quy định;

- Tổng hợp các Đề án, Dự án về bảo đảm an toàn thông tin mạng của các phòng, đơn vị; Chủ trì, phối hợp các đơn vị liên quan tham mưu Lãnh đạo Thanh tra tỉnh xây dựng dự trù kinh phí thực hiện các Đề án, Dự án về bảo đảm an toàn thông tin mạng (nếu có);

- Chủ trì, phối hợp với các cơ quan, đơn vị liên quan thanh tra, kiểm tra định kỳ hoặc đột xuất; kịp thời phát hiện và xử lý theo thẩm quyền đối với các hành vi vi phạm an toàn thông tin mạng trong phạm vi của Thanh tra tỉnh;

- Tuyên truyền, cử cán bộ tham gia các khóa đào tạo, hội nghị tuyên truyền về an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước do Sở Thông tin và Truyền thông tổ chức;

- Hướng dẫn về nghiệp vụ quản lý vận hành, kỹ thuật bảo đảm an toàn thông tin mạng; hỗ trợ giải quyết sự cố khi có yêu cầu;

- Hướng dẫn, giám sát các các đơn vị xây dựng quy định nội bộ và thực hiện việc bảo đảm an toàn thông tin mạng cho hệ thống thông tin theo quy định của Nhà nước;

- Tham gia mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia và thực hiện trách nhiệm, quyền hạn của thành viên mạng lưới ứng cứu an toàn thông tin mạng quốc gia theo quy định tại Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 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;

- Hàng năm, Văn phòng căn cứ kết quả kiểm tra, đánh giá, báo cáo công tác bảo đảm an toàn thông tin mạng của các đơn vị, đề xuất Lãnh đạo Thanh tra

tỉnh xem xét khen thưởng cho các cá nhân, đơn vị có nhiều thành tích trong công tác bảo đảm an toàn thông tin mạng theo quy định hiện hành;

- Tổng hợp và báo cáo về tình hình an toàn thông tin mạng theo định kỳ gửi Sở Thông tin và Truyền thông và các cơ quan, đơn vị có liên quan;

- Trách nhiệm phối hợp tại Điều 5 Quy chế này;

- Chủ trì, phối hợp với các phòng Nghiệp vụ đôn đốc, hướng dẫn triển khai nghiêm túc Quy chế này.

2. Các phòng Nghiệp vụ thuộc Thanh tra tỉnh

- Trưởng các phòng Nghiệp vụ, Chánh Văn phòng thuộc đối tượng áp dụng của Quy chế này có trách nhiệm: Phổ biến, triển khai tới toàn thể công chức, người lao động của phòng, tổ chức thực hiện công tác bảo đảm an toàn thông tin mạng; chịu trách nhiệm trước pháp luật và Lãnh đạo Thanh tra tỉnh về các vi phạm trong việc bảo đảm an toàn thông tin mạng cho các hệ thống thông tin của Thanh tra tỉnh được giao quản lý, sử dụng.

- Phối hợp với Văn phòng Thanh tra tỉnh và các đơn vị có liên quan kiểm tra, kiểm soát về an toàn thông tin mạng; kịp thời xử lý các tập thể, cá nhân vi phạm pháp luật về an toàn thông tin mạng; phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống thông tin của Thanh tra tỉnh, gây phương hại đến an ninh quốc gia, gây mất an ninh trật tự và an toàn xã hội theo thẩm quyền.

3. Cán bộ, công chức, người lao động thuộc Thanh tra tỉnh có trách nhiệm: Tuân thủ Quy chế; thông báo các vấn đề bất thường liên quan tới an toàn an ninh mạng cho bộ phận chuyên trách chuyên trách an toàn an ninh mạng; chịu trách nhiệm trước pháp luật và Lãnh đạo cơ quan về các vi phạm, an toàn thông tin mạng do không tuân thủ Quy chế.

Điều 26. Rà soát, cập nhật, bổ sung Quy chế

1. Định kỳ 03 năm hoặc khi có thay đổi về căn cứ pháp lý về bảo đảm an toàn thông tin, bộ phận chuyên trách an toàn thông tin (Văn phòng Thanh tra tỉnh) kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung báo cáo Chánh Thanh tra xem xét, quyết định.

2. Trong quá trình thực hiện Quy chế, nếu có vấn đề vướng mắc, phát sinh, các phòng Nghiệp vụ phản ánh kịp thời về bộ phận chuyên trách an toàn thông tin (Văn phòng Thanh tra tỉnh) để tổng hợp báo cáo Lãnh đạo Thanh tra tỉnh xem xét, điều chỉnh bổ sung cho phù hợp./.

PHỤ LỤC 1
Mẫu số 03 theo Thông tư số 20/2017/TT-BTTT ngày 12/9/2017
của Bộ Thông tin và Truyền thông

BÁO CÁO BAN ĐẦU SỰ CỐ MẠNG

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 hệ thống thông tin (*):	*Điền tên đơn vị vận hành hoặc được thuê vận hành hệ thống thông tin*				
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 hệ thống thông tin (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*				
Điền tên nhà cung cấp ở đây	*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 gian 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 *

□ Thành viên mạng lưới chịu trách nhiệm ứng cứu sự cố cho tổ chức, cá nhân

□ ISP đang trực tiếp cung cấp dịch vụ

□ Cơ quan điều phối

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 an toàn thông tin 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, 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)

CÁ NHÂN/NGƯỜI ĐẠI DIỆN THEO PHÁP LUẬT
(Ký tên, đóng dấu)

Chú thích: 1. Phần (*) là những thông tin bắt buộc. Các phần còn lại có thể loại bỏ nếu không có thông tin.

2. Sử dụng tiêu đề (subject) bắt đầu bằng "[TBSC]" khi gửi thông báo qua email

3. Tham khảo thêm tại website của VNCERT (www.vncert.gov.vn)

PHỤ LỤC 2
Mẫu số 04 theo Thông tư số 20/2017/TT-BTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông

BÁO CÁO KẾT THÚC ỨNG PHÓ SỰ CỐ THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN BÁO CÁO

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

▪ Địa chỉ: (*) .....

▪ Điện thoại (*)…….. Email (*).....

KÝ HIỆU BÁO CÁO BAN ĐẦU SỰ CỐ: Số ký hiệu …….. Ngày báo cáo: / /201...

THÔNG TIN CHI TIẾT VỀ HỆ THỐNG BỊ SỰ CỐ

Tên đơn vị vận hành hệ thống thông tin (*):	*Điền tên đơn vị vận hành hoặc được thuê vận hành hệ thống thông tin*				
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 hệ thống thông tin, (nếu có)	□ Cấp độ 1	□ Cấp độ 2	□ Cấp độ 3	□ Cấp độ 4	□ Cấp độ 5

Tên/Mô tả về sự cố

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.....)

CÁ NHÂN/NGƯỜI ĐẠI DIỆN THEO PHÁP LUẬT
(Ký tên, đóng dấu)