UBND TỈNH BÌNH ĐỊNH **SỞ CÔNG THƯƠNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 214 /QĐ-SCT	*Bình Định, ngày 31 tháng 12 năm 2021*

QUYẾT ĐỊNH

Về việc ban hành Quy chế đảm bảo an toàn thông tin mạng trong triển khai chính quyền điện tử, chính quyền số của Sở Công Thương

GIÁM ĐỐC SỞ CÔNG THƯƠNG

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

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

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

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

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

Căn cứ Quyết định số 22/2021/QĐ-UBND ngày 11 tháng 6 năm 2021 của Ủy ban nhân dân tỉnh Bình Định về việc ban hành Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Bình Định;

Căn cứ Quyết định số 3501/QĐ-UBND ngày 08 tháng 10 năm 2015 của UBND tỉnh Bình Định về việc ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Công Thương; Quyết định số 2959/QĐ-UBND ngày 24 tháng 7 năm 2020 của UBND tỉnh sửa đổi một số điều của Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Công Thương ban hành kèm theo Quyết định số 3501/QĐ-UBND ngày 08/10/2015 của UBND tỉnh;

Theo đề nghị của Chánh Văn phòng Sở.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn thông tin mạng trong trong triển khai chính quyền điện tử, chính quyền số của Sở Công Thương.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký và thay thế Quyết định số 140/QĐ-SCT ngày 22/10/2014 của Sở Công Thương về việc ban hành Quy chế đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin Sở Công Thương.

Điều 3. Chánh Văn phòng, người đứng đầu các phòng, đơn vị thuộc Sở và đơn vị trực thuộc Sở; công chức, viên chức, người lao động thuộc Sở chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như điều 3;
- Lãnh đạo Sở;
- Các phòng, đơn vị thuộc Sở;
- ĐVTT Sở;
- Lưu: VT, VP.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ CÔNG THƯƠNG
TỈNH BÌNH ĐỊNH

Ngô Văn Tổng

UBND TỈNH BÌNH ĐỊNH
SỞ CÔNG THƯƠNG

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

QUY CHẾ
Đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin, triển khai chính quyền điện tử, chính quyền số Sở Công Thương Bình Định

(Ban hành kèm theo Quyết định số: 214 /QĐ-SCT ngày 31 /12/2021 của Sở Công Thương Bình Định)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định biện pháp, chính sách quản lý nhằm bảo đảm an toàn thông tin các hệ thống thông tin trong hoạt động ứng dụng công nghệ thông tin, triển khai chính quyền điện tử, chính quyền số của Sở Công Thương.

Điều 2. Đối tượng áp dụng

Quy chế này áp dụng đối với các phòng, đơn vị thuộc Sở, đơn vị trực thuộc Sở và công chức, viên chức, người lao động thuộc Sở Công Thương.

Điều 3. Giải thích từ ngữ

1. An toàn thông tin mạng là công tác bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

2. Hệ thống thông tin (viết tắt là 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 của một cơ quan, tổ chức.

3. Chủ quản hệ thống thông tin là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin.

4. Đơn vị vận hành hệ thống thông tin là cơ quan, tổ chức được chủ quản hệ thống thông tin giao nhiệm vụ vận hành hệ thống thông tin. Trong trường hợp chủ quản hệ thống thông tin thuê ngoài dịch vụ công nghệ thông tin, đơn vị vận hành hệ thống thông tin là bên cung cấp dịch vụ.

5. 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.

6. 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.

7. Mạng ngang hàng là mô hình mạng mà trong đó các máy tính có quyền bình đẳng như nhau, mỗi máy tính có quyền chia sẻ tài nguyên và sử dụng các tài nguyên từ máy tính khác.

8. Đơn vị chuyên trách về công nghệ thông tin là đơn vị chuyên trách về công nghệ thông tin của chủ quản hệ thống thông tin do chủ quản hệ thống thông tin chỉ định.

9. Đơn vị chuyên trách về an toàn thông tin là đơn vị có chức năng, nhiệm vụ bảo đảm an toàn thông tin của chủ quản hệ thống thông tin.

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

Điều 4. Nguyên tắc bảo đảm an toàn thông tin

1. Hoạt động ứng dụng công nghệ thông tin, triển khai chính quyền điện tử, chính quyền số phải bảo đảm an toàn thông tin mạng. Hoạt động an toàn thông tin mạng phải đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước, giữ vững ổn định chính trị, trật tự, an toàn xã hội và thúc đẩy phát triển kinh tế - xã hội.

2. Công chức, viên chức, người lao động Sở Công Thương không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác.

3. Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, thông tin riêng của tổ chức.

4. Hoạt động an toàn thông tin mạng phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.

Chương II
QUY ĐỊNH ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 5. Yêu cầu thiết kế, xây dựng hệ thống thông tin.

1. Khi thiết kế xây dựng, nâng cấp, mở rộng hệ thống thông tin, phòng, đơn vị thuộc Sở được giao chủ trì tham mưu xây dựng, nâng cấp, mở rộng hệ thống thông tin của Sở Công Thương phối hợp với đơn vị tư vấn xây dựng tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin; xây dựng tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin; xây dựng tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin; xây dựng phương án bảo đảm an toàn thông tin phù hợp với cấp độ an toàn thông tin của cơ quan và gửi đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin thẩm định (hoặc đơn vị chuyên trách về an toàn thông tin của Ủy ban nhân dân tỉnh) trước khi trình cấp có thẩm quyền phê duyệt dự án.

2. Trước khi đưa vào vận hành, khai thác hệ thống thông tin, phòng, đơn vị

thuộc Sở được giao chủ trì tham mưu xây dựng, nâng cấp, mở rộng hệ thống thông tin của Sở Công Thương phải thực hiện kiểm thử hoặc vận hành thử trước khi đưa vào sử dụng. Kết quả kiểm thử, vận hành thử phải được lập thành văn bản và tuân thủ theo quy định tại Điều 10 Thông tư số 24/2020/TT-BTTTT ngày 09/9/2020 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về công tác triển khai, giám sát công tác triển khai và nghiệm thu dự án đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước.

Điều 6. Quản lý thuê dịch vụ công nghệ thông tin

1. Khi ký kết hợp đồng thuê dịch vụ công nghệ thông tin, phòng, đơn vị thuộc Sở được giao chủ trì sử dụng dịch vụ phải tham mưu Sở Công Thương phải xác định rõ phạm vi, trách nhiệm, quyền hạn và nghĩa vụ của các bên về bảo đảm an toàn thông tin. Trong hợp đồng phải bao gồm các điều khoản về việc xử lý vi phạm quy định bảo đảm an toàn thông tin và trách nhiệm bồi thường thiệt hại do hành vi vi phạm của bên cung cấp dịch vụ gây ra.

2. Trách nhiệm của phòng, đơn vị thuộc Sở được giao chủ trì sử dụng dịch vụ trong quá trình sử dụng dịch vụ công nghệ thông tin

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 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 an toàn thông tin 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 hệ thống thông tin của Sở Công Thương.

3. Trách nhiệm của phòng, đơn vị thuộc Sở được giao chủ trì sử dụng dịch vụ khi phát hiện bên cung cấp dịch vụ có dấu hiệu vi phạm quy định bảo đảm an toàn thông tin:

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 hệ thống thông tin 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. Trách nhiệm của phòng, đơn vị thuộc Sở được giao chủ trì sử dụng dịch vụ khi kết thúc sử dụng dịch vụ

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

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, đơn vị 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 7. Bảo vệ bí mật nhà nước trong hoạt động ứng dụng công nghệ thông tin

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

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

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

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

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

3. Trước khi thanh lý các máy tính trong các cơ quan nhà nước, đơn vị được giao vận hành HTTT của Sở phải dùng các biện pháp kỹ thuật xoá bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

Điều 8. Quy định về cấp phát, thu hồi, cập nhật và quản lý các tài khoản truy cập vào hệ thống thông tin

1. Trách nhiệm, quyền hạn người dùng khi truy cập, đăng nhập các hệ thống thông tin: đảm bảo mỗi người dùng khi sử dụng hệ thống thông tin phải được cấp và sử dụng tài khoản truy cập với định danh duy nhất gắn với người dùng đó; trường hợp sử dụng tài khoản dùng chung cho một nhóm người hay một đơn vị, phải có cơ chế xác định cá nhân, đơn vị có trách nhiệm quản lý tài khoản. Người dùng chỉ được truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình và có trách nhiệm bảo mật tài khoản truy cập được cấp.

2. Đơn vị được giao vận hành HTTT của Sở thực hiện quản lý, cấp tài khoản cá nhân và phân quyền truy cập cho người sử dụng. Trong trường hợp cần thiết có thể hủy tài khoản truy cập cá nhân và ngắt kết nối đối với các hành vi cố ý tấn công hoặc gây trở ngại cho mạng máy tính; hủy quyền truy cập hệ thống thông tin đối với công chức, viên chức (CCVC) nghỉ chế độ, chuyển công tác và đảm bảo cơ quan vẫn truy nhập được vào các hồ sơ được tạo ra bởi CCVC đó. Hướng dẫn người sử dụng thay đổi mật khẩu ngay sau khi đăng nhập lần đầu tiên và bảo vệ thông tin của tài khoản theo quy định.

3. Mật mã đăng nhập, truy cập hệ thống thông tin phải có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặc

biệt như !, @, #, $, %,...).

Điều 9. Bảo đảm nguồn nhân lực

1. Khi tuyển dụng cán bộ chuyên trách an toàn thông tin/ công nghệ thông tin của phải xây dựng các quy định đối với công tác tuyển dụng. Người được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng.

2. Cán bộ chuyên trách 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.

3. Người 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 được quy định; 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 người có thẩm quyền để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm.

4. Đơn vị được giao vận hành HTTT của Sở 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 tổ chức cá nhân sử dụng hệ thống thông tin do đơn vị quản lý.

Điều 10. Bảo đảm an toàn hạ tầng mạng

1. Quản lý hạ tầng mạng nội bộ:

a) Đơn vị được giao vận hành HTTT của Sở 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 công nghệ thông tin của các cơ quan nhà nước, bảo đảm an toàn thông tin; hạn chế sử dụng mô hình mạng có nguy cơ mất an toàn thông tin cao.

b) Tổ chức mô hình mạng: Cài đặt, cấu hình, tổ chức hệ thống mạng theo mô hình Máy khách/Máy chủ (Client/Server), hạn chế sử dụng mô hình mạng ngang hàng. 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, đơn vị khi kết nối với hệ thống bên ngoài; Xây dựng hoặc thuê hệ thống giám sát an toàn thông tin để kiểm soát, phát hiện truy cập trái phép vào hệ thống.

c) Đối với các phòng, ban, đơn vị trực thuộc không nằm cùng một khu vực thì cần thiết lập mạng riêng ảo (VPN) để tăng cường an ninh cho hạ tầng mạng nội bộ. Khi thiết lập các dịch vụ trên môi trường mạng Internet, chỉ cung cấp những chức năng thiết yếu nhất bảo đảm duy trì hoạt động của hệ thống thông tin; hạn chế sử dụng/mở cổng giao tiếp mạng, giao thức và các dịch vụ không cần thiết.

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.

đ) Xây dựng 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 trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác.

e). Không tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập không dây của cá nhân vào mạng nội bộ của Sở.

g) Không tự ý thay đổi, gỡ bỏ biện pháp, giải pháp an toàn thông tin cài đặt trên thiết bị công nghệ thông tin phục vụ công việc; tự ý thay thế, lắp mới, tráo đổi thành phần của máy tính phục vụ công việc. Cá nhân, tổ chức phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng.

2. Quản lý hệ thống 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 được giao vận hành HTTT của Sở phải thiết lập các tham số: Tên, nhận dạng dịch vụ (Service Set Identifier - SSID), mật khẩu 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: !, @, #, $, %), 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 6 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, Đơn vị được giao vận hành HTTT của Sở phải tạo thêm một SSID riêng và giới hạn băng thông truy cập phù hợp đối với đối tượng này.

Điều 11. Bảo đảm an toàn máy chủ và ứng dụng

1. Trên hệ thống máy chủ

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 Sở Công Thương, không cài đặt các dịch vụ không sử dụng;

b) Thiết lập chế độ tự động cập nhật phiên bản và 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 (Basic Input/Output System), trong đó lưu ý việc vô hiệu hóa các cổng USB trên máy chủ.

d) Xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng.

2. Trang bị phần mềm phòng chống mã độc (antivirus) có bản quyền cho hệ thống máy chủ; 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 hằng tuần.

3. Định kỳ hằng tuần, đơn vị được giao vận hành HTTT của Sở 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 tệp tin lưu trữ sự kiện (logfile): Đơn vị được giao vận hành HTTT của Sở 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 06 tháng kiểm tra, bảo đảm tính toàn vẹn của các logfile, hạn chế tình trạng tràn logfile gây ảnh hưởng đến hoạt động của hệ thống thông tin.

5. Quản lý phiên bản: Đơn vị được giao vận hành HTTT của Sở xây dựng nhật ký quản lý phiên bản hệ thống thông tin bao gồm các thông tin: Chủ đầu tư, tên hệ thống thông tin, 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 hệ thống thông tin tại hệ thống lưu trữ độc lập.

6. Khi thiết lập cung cấp các dịch vụ ra môi trường mạng (tuân thủ theo TCP/UDP Port), đơn vị được giao vận hành HTTT của Sở 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).

Điều 12. 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 được giao vận hành HTTT của Sở phải thông báo và người dùng phải thay đổi mật khẩu sau khi đăng nhập thành công lần đầu;

b) Các hệ thống thông tin 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 hệ thống thông tin xác lập chế độ thoát ra khỏi hệ thống nếu người sử dụng không tương tác trên hệ thống của phiên làm việc quá 20 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 (ví dụ tài khoản thư điện tử, chữ ký số, chứng thư số) để đăng nhập vào hệ thống thông tin, cơ sở dữ liệu;

d) Tài khoản thư điện tử, chữ ký số chuyên dùng (xx@sct.binhdinh.gov.vn và chữ ký số do Ban Cơ yếu Chính phủ cấp) 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; định kỳ 01 năm kiểm tra việc lưu trữ của hệ

thống thư điện tử, tiến hành xóa các mail quá cũ, không cần thiết để đảm bảo hệ thống hoạt động ổn định thông suốt;

đ) Tài khoản quản trị hệ thống được giao cho đơn vị vận hành HTTT của Sở phục vụ cho công tác quản trị, phân quyền, cấu hình hệ thống đó; đơn vị được giao vận hành HTTT của Sở không sử dụng cùng một mật khẩu cho nhiều tài khoản khác nhau;

e) 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 được giao vận hành HTTT của Sở điều chỉnh, thu hồi, hủy bỏ tài khoản, chữ ký số, chứng thư số.

2. Cơ chế mã hóa và sao lưu dữ liệu phải đảm bảo tính toàn vẹn của dữ liệu.

3. 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; 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.

4. Đối với công tác 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):

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

b) Xây dựng tài liệu, quy trình hướng dẫn sao lưu/phục hồi dữ liệu của hệ thống: đơn vị được giao vận hành HTTT của Sở xây dựng tài liệu hướng dẫn sao lưu cụ thể đối với từng hệ thống cung cấp dịch vụ, hệ thống điều hành của Sở.

5. Đơn vị được giao vận hành HTTT của Sở phối hợp với các đơn vị có liên quan thực hiện xác định các thông tin, thực hiện quy trình sao lưu dự phòng và phục hồi cho các phần mềm, dữ liệu cần thiết theo quy định, quy trình sao lưu, lưu trữ. Các nội dung thực hiện gồm: thông tin cấu hình của mạng, máy chủ, phần mềm ứng dụng, cơ sở dữ liệu, tệp tin ghi nhật ký hệ thống; 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; thực hiện quy trình sao lưu dự phòng và phục hồi.

6. Dữ liệu sao lưu phải được lưu trữ an toàn trên Hệ thống lưu trữ dự phòng, thiết bị lưu trữ ngoài và được kiểm tra thường xuyên đảm bảo sẵn sàng cho việc sử dụng khi cần; việc kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu tối thiểu 6 tháng một lần (hoặc khi có yêu cầu đột xuất).

7. Các tên miền (bao gồm cả tên miền *.sct.binhdinh.gov.vn) khi không còn sử dụng, đơn vị được giao vận hành HTTT của Sở tham mưu Sở có văn bản gửi đến Sở Thông tin và Truyền thông, Trung Tâm Internet Việt Nam (VNNIC)

để đề nghị hủy tên miền; các hệ thống thông tin không sử dụng, chủ quản hệ thống thông tin 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 cơ quan, đơn vị cung cấp dịch vụ lưu ký xóa hoàn toàn dữ liệu trên các máy chủ.

8. Khi thực hiện chia sẻ tài nguyên trên máy chủ hoặc máy trạm, 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. Các thông tin, tài liệu, dữ liệu nhạy cảm phải được mã hóa trước khi trao đổi, truyền nhận qua mạng máy tính.

9. Đơn vị quản lý máy chủ, máy trạm và thiết bị lưu trữ khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài Sở phải tháo rời bộ phận lưu trữ khỏi thiết bị và để lại Sở 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.

10. 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.

11. Định kỳ 3 năm 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. Bản sao lưu được lưu trữ tối thiểu thành 02 bản và được lưu trữ ở hai địa chỉ khác nhau.

Điều 13. Bảo đảm an toàn thiết bị đầu cuối

1. Trên máy tính cá nhân phải thiết lập chế độ tự động cập nhật hệ điều hành trên máy tính, phải thiết lập mật khẩu truy nhập chế độ tự động bảo vệ màn hình khi không sử dụng; sử dụng những trình duyệt an toàn, đáng tin cậy, cài đặt phần mềm phòng chống mã độc; 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 hằng tuần.

2. Khuyến khích đầu tư, mua sắm thiết bị công nghệ thông tin sản xuất trong nước.

3. Kết nối máy tính/thiết bị đầu cuối của người sử dụng vào hệ thống:

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 Sở;

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 đơn vị được giao vận hành HTTT của Sở.

3. Trong quá trình sử dụng thiết bị đầu cuối:

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 đơn vị được giao vận hành HTTT của Sở để kịp thời ngăn chặn và xử lý.

Điều 14. Quản lý giám sát an toàn hệ thống thông tin

1. Hệ thống thông tin phải phải được triển khai hệ thống giám sát an toàn thông tin đáp ứng các yêu cầu 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.

2. Đối với các hệ thống thông tin, phần mềm, ứng dụng, cơ sở dữ liệu không được đặt tại Trung tâm tích hợp dữ liệu tỉnh thì yêu cầu doanh nghiệp cung cấp dịch vụ bảo đảm các yêu cầu giám sát an toàn hệ thống thông tin theo quy định của pháp luật.

4. Định kỳ hàng năm tổ chức đánh giá, kiểm tra đối với hệ thống thông tin nội bộ tại cơ quan. Thực hiện các biện pháp bảo trì cần thiết để bảo đảm khả năng xử lý và tính sẵn sàng của hệ thống thông tin.

Điều 15. Ứng cứu 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 an toàn thông tin;

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 đơn vị vận hành hệ thống thông tin;

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

2. Phân nhóm sự cố an toàn thông tin:

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

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

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

d) Sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn. Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin: Hoạt động ứng cứu sự cố an toàn thông tin mạng huy động các nguồn lực nằm ngoài phạm vi của đơn vị vận hành hệ thống thông tin để đối phó với các sự cố quy định tại khoản 1 điều này.

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 Sở Công Thương;

b) Trung bình: Sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của Sở Công Thương;

c) Cao: Sự cố tác động đến khả năng vận hành của hệ thống thông tin, ảnh hưởng đến dữ liệu, thiết bị, gây ảnh hưởng đến hoạt động chung của Sở Công Thương 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 Sở Công Thương và 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 Sở Công Thương và người dân, doanh nghiệp, đe dọa trật tự an toàn xã hội.

4. Phương án tiếp nhận và quy trình phối hợp ứng cứu xử lý sự cố

a) Phương án tiếp nhận

- Sở Công Thương thông báo công khai thông tin, địa chỉ của đơn vị được giao vận hành HTTT của Sở để tiếp nhận thông tin sự cố an toàn thông tin mạng liên quan đến HTTT của Sở Công Thương.

- Khi phát hiện sự cố an toàn thông tin mạng liên quan đến HTTT của Sở Công Thương, cá nhân, tập thể phát hiện sự cố thông báo ngay cho đơn vị được giao vận hành HTTT của Sở Công Thương.

- Đơn vị được giao vận hành HTTT của Sở Công Thương chủ động tiếp nhận các nội dung như:

+ Tên, địa chỉ cá nhân, tập thể Đơn vị vận hành hệ thống thông tin; cơ quan chủ quản hệ thống thông tin; hệ thống thông tin bị sự cố; thời điểm phát hiện sự cố;

+ Đầu mối liên lạc về sự cố của đơn vị vận hành hệ thống bị sự cố: Tên, chức vụ, điện thoại, thư điện tử;

+ Mô tả về sự cố: Loại sự cố, hiện tượng, đánh giá sơ bộ mức độ nguy hại, mức độ lây lan, tác động của sự cố đến hoạt động bình thường của tổ chức;

+ Đơn vị cung cấp dịch vụ hạ tầng công nghệ thông tin, viễn thông;

+ Liệt kê các biện pháp đã triển khai hoặc dự kiến triển khai để xử lý khắc phục sự cố;

+ Các tổ chức, doanh nghiệp đang hỗ trợ ứng cứu, xử lý và kết quả xử lý sự cố tính đến thời điểm báo cáo;

+ Kết quả ứng cứu sự cố ban đầu;

+ Kiến nghị đề xuất hướng ứng cứu xử lý sự cố (nếu có);

- Đơn vị được giao vận hành HTTT của Sở Công Thương thực hiện: Phân

nhóm sự cố an toàn thông tin; phân loại mức độ nghiêm trọng sự cố và thực hiện theo quy trình phối hợp ứng cứu xử lý sự cố

b) Quy trình phối hợp ứng cứu xử lý sự cố

- Bước 1: Nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc thẩm quyền Sở Công Thương 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 tích hợp Dữ liệu tỉnh) thì thực hiện tiếp Bước 3;

- Bước 2: Tiến hành xử lý sự cố; Trường hợp sự cố được khắc phục thì lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố; trường hợp sự cố vượt quá khả năng xử lý thì lập biên bản ghi nhận và thực hiện tiếp Bước 3;

- Bước 3: Báo sự cố đến Sở Thông tin và Truyền thông theo mẫu số 01 kèm theo Quy chế;

- 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, đơn vị, tổ chức có liên quan để tiến hành khắc phục sự cố và thực hiện tiếp Bước 5;

- Bước 5: Lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố theo mẫu số 02 kèm theo Quy chế này. Lãnh đạo Sở Công Thương 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.

5. Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục, Đơn vị được giao vận hành HTTT của Sở Công Thương tham mưu Sở Công Thương báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ.

6. Trách nhiệm của đơn vị được giao vận hành HTTT của Sở Công Thương

a) 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 theo quy trình phối hợp ứng cứu xử lý sự cố tại khoản 4 và 5 Điều 15.

c) 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.

d) Xây dựng kế hoạch và tổ chức diễn tập phương án xử lý sự cố an toàn thông tin.

Chương III
KIỂM TRA, ĐÁNH GIA CÔNG TÁC ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 16. Kế hoạch kiểm tra hằng năm

1. Đơn vị được giao vận hành HTTT của Sở chủ trì, phối hợp với các đơn vị liên quan xây dựng Kế hoạch và triển khai thực hiện kiểm tra công tác đảm bảo an toàn thông tin đối với các phòng, đơn vị thuộc Sở, đơn vị trực thuộc Sở hằng năm.

2. Tiến hành kiểm tra đột xuất các các phòng, đơn vị khi có dấu hiệu vi phạm an toàn đối với các hệ thống thông tin của Sở.

Điều 17. Nội dung, hình thức kiểm tra, đánh giá hệ thống thông tin

1. Nội dung kiểm tra, đánh giá:

a) Kiểm tra việc thực theo các nội dung theo Quy chế này; việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin; Kiểm tra hiệu quả của các biện pháp bảo đảm an toàn thông tin;

b) Đánh giá hiệu quả của biện pháp bảo đảm an toàn hệ thống thông tin; phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống;

2. Hình thức kiểm tra, đánh giá:

a) Kiểm tra, đánh giá định kỳ theo kế hoạch của Sở Công Thương.

b) Kiểm tra, đánh giá đột xuất theo yêu cầu của cấp có thẩm quyền.

3. Cấp có thẩm quyền yêu cầu kiểm tra, đánh giá:

a) Đơn vị chuyên trách ATTT tại Trung ương;

b) Ủy ban nhân dân tỉnh hoặc Sở Thông tin và Truyền thông (đơn vị chuyên trách về an toàn thông tin trên địa bàn tỉnh);

c) Giám đốc Sở Công Thương.

4. Đơn vị chủ trì kiểm tra, đánh giá là đơn vị được cấp có thẩm quyền giao nhiệm vụ hoặc được lựa chọn để thực hiện nhiệm vụ kiểm tra, đánh giá.

5. Đối tượng kiểm tra, đánh giá là các phòng, đơn vị thuộc Sở, đơn vị trực thuộc Sở.

Chương IV
TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG VÀ TỔ CHỨC THỰC HIỆN

Điều 18. Trách nhiệm của Văn phòng Sở

1. Tham mưu, đề xuất Giám đốc Sở công tác bảo đảm an toàn thông tin tại Sở Công Thương và chịu trách nhiệm trước Giám đốc Sở trong việc bảo đảm an toàn thông tin tại cơ quan.

2. Hằng năm, chủ trì, phối hợp với các đơn vị liên quan tuyên truyền, phổ biến, quán triệt các quy định về an toàn thông tin; kiểm tra công tác bảo đảm an toàn thông tin mạng trong phạm vi Sở Công Thương.

3. Hằng năm, đề xuất Giám đốc Sở cử công chức, viên chức phụ trách công nghệ thông tin của các phòng, đơn vị bồi dưỡng, tập huấn về công tác bảo đảm an toàn thông tin mạng, tham dự các hội nghị, hội thảo chuyên đề về an toàn thông tin mạng do các cơ quan liên quan tổ chức.

4. Tham mưu Lãnh đạo Sở phối hợp với Công an tỉnh, Sở Thông tin và Truyền thông và các cơ quan có liên quan có các biện pháp phòng, chống các thông tin vi phạm pháp luật, ảnh hưởng đến an ninh quốc gia, trật tự, an toàn xã hội trên môi trường mạng, nhất là trên Trang TTĐT Sở Công Thương.

5. Là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin; tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng tại Sở Công Thương.

6. Hằng năm xây dựng dự toán kinh phí cho việc ứng dụng công nghệ thông tin nói chung và công tác bảo đảm an toàn thông tin mạng nói riêng tại Sở Công Thương; lập kế hoạch nâng cấp, bảo trì, sửa chữa, gia hạn bản quyền phần mềm... cho các hệ thống phần cứng, phần mềm nhằm thực hiện tốt công tác bảo mật, bảo đảm an toàn thông tin mạng đưa vào dự toán chi năm sau để triển khai thực hiện.

Điều 19. Trách nhiệm của các phòng, đơn vị thuộc Sở và đơn vị trực thuộc Sở.

1. Người đứng đầu các phòng, đơn vị thuộc Sở và đơn vị trực thuộc Sở có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trong công tác bảo đảm an toàn thông tin mạng của phòng, đơn vị mình.

2. Phân công công chức, viên chức phụ trách công nghệ thông tin bảo đảm an toàn thông tin của phòng, đơn vị; chỉ đạo công chức, viên chức và người lao động nghiêm túc chấp hành các quy định về bảo đảm an toàn thông tin; tạo điều kiện để các công chức, viên chức phụ trách công nghệ thông tin được học tập, nâng cao trình độ về an toàn thông tin; thường xuyên tổ chức quán triệt các quy định về an toàn thông tin trong phòng, đơn vị.

3. Phối hợp, cung cấp thông tin và tạo điều kiện cho các phòng, đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố xảy ra một cách kịp thời, nhanh chóng và đạt hiệu quả.

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

Điều 20. Trách nhiệm của công chức, viên chức và người lao động

1. Trách nhiệm của công chức, viên chức phụ trách về an toàn thông tin/công nghệ thông tin tại cơ quan, đơn vị

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

b) Thực hiện việc giám sát, đánh giá, báo cáo Người đứng đầu cơ quan, đơn vị các rủi ro mất an toàn thông tin mạng và mức độ nghiêm trọng của các

rủi ro đó.

c) 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 thông tin mạng.

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

2. Trách nhiệm của người sử dụng

a) Nghiêm túc chấp hành 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) 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 đầy đủ các chương trình bồi dưỡng, tập huấn về an toàn thông tin mạng khi được phân công.

Điều 21. Tổ chức thực hiện

1. Căn cứ Quy chế này, Người đứng đầu các phòng, đơn vị thuộc Sở và đơn vị trực thuộc Sở có trách nhiệm tổ chức triển khai thực hiện Quy chế này.

2. Giao Văn phòng Sở theo dõi, triển khai việc thực hiện Quy chế này. Định kỳ tổng hợp báo cáo Giám đốc Sở tình hình thực hiện đảm bảo an toàn thông tin mạng tại các phòng, đơn vị theo quy định.

3. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc các phòng, đơn vị tổng hợp phản ánh gửi về Sở (qua Văn phòng Sở), trình Giám đốc Sở xem xét, sửa đổi bổ sung cho phù hợp./.

MẪU SỐ 01

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*				
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 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 PHÁT LUẬT

(Ký tên, đóng dấu)

MẪU SỐ 02

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 PHÁT LUẬT

(Ký tên, đóng dấu)