ỦY BAN NHÂN DÂN TỈNH HẢI DƯƠNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 39 /2024/QĐ-UBND	*Hải Dương, ngày 13 tháng 9 năm 2024*

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Hải Dương

ỦY BAN NHÂN DÂN TỈNH HẢI DƯƠNG

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19 tháng 6 năm 2015; Luật sửa đổi, bổ sung một số điều của Luật Tổ chức Chính phủ và Luật Tổ chức chính quyền địa phương ngày 22 tháng 11 năm 2019;

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 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 72/2013/NĐ-CP ngày 15 tháng 7 năm 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 tháng 7 năm 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 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 27/2017/TT-BTTTT ngày 20 tháng 10 năm 2017 của Bộ trưởng 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; Thông tư số 12/2019/TT-BTTTT ngày 05 tháng 11 năm 2019 sửa đổi, bổ sung một số điều của Thông tư số 27/2017/TT-BTTTT ngày 20 tháng 10 năm 2017 của Bộ trưởng 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 Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ trưởng Bộ trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;

Căn cứ Thông tư số 24/2020/TT-BTTTT ngày 09 tháng 9 năm 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;

Căn cứ Thông tư 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 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;

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông.

QUYẾT ĐỊNH:

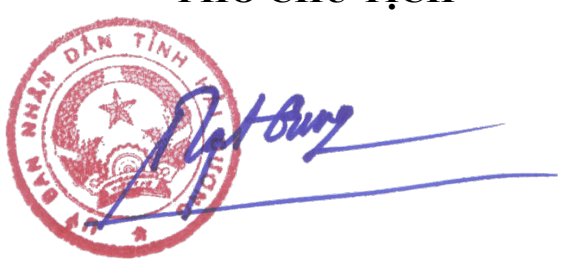
Điều 1. Ban hành kèm theo Quyết định này "Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Hải Dương".

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày 25 tháng 9 năm 2024 và thay thế Quyết định số 29/2013/QĐ-UBND ngày 11 tháng 12 năm 2013 của Ủy ban nhân dân tỉnh Hải Dương về việc ban hành Quy chế bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước trên địa bàn tỉnh Hải Dương.

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh; Thủ trưởng các sở, ban, ngành của tỉnh; Chủ tịch Ủy ban nhân dân các huyện, thị xã, thành phố và tổ chức, cá nhân liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Văn phòng Chính phủ;
- Vụ pháp chế - Bộ Thông tin và Truyền thông;
- Cục Kiểm tra văn bản QPPL- Bộ Tư pháp;
- Thường trực Tỉnh ủy, TT HĐND tỉnh;
- Ban chỉ đạo Chuyển đổi số tỉnh;
- Chủ tịch, các PCT UBND tỉnh;
- Báo Hải Dương, Đài PTTH tỉnh;
- Phòng HC-QT - VP UBND tỉnh;
- Trung tâm CNTT - VP UBND tỉnh;
- Lưu: VT, KGVX, Nam(01b)

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



Nguyễn Minh Hùng

ỦY BAN NHÂN DÂN TỈNH HẢI DƯƠNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY CHẾ
Bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Hải Dương

(Ban hành kèm theo Quyết định số 39 /2024/QĐ-UBND ngày 13 tháng 9 năm 2024 của Ủy ban nhân dân tỉnh Hải Dương)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Hải Dương.

Điều 2. Đối tượng áp dụng

1. Quy chế này được áp dụng đối với các cơ quan nhà nước tỉnh Hải Dương và các tổ chức, cá nhân liên quan đến hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Hải Dương.

2. Các tổ chức, cá nhân, doanh nghiệp có tham gia quản lý, cung cấp, vận hành, khai thác, ứng dụng công nghệ thông tin trong hoạt động của các cơ quan, đơn vị nêu tại khoản 1 Điều này.

3. Cán bộ, công chức, viên chức, người lao động đang công tác trong các cơ quan, đơn vị nêu tại khoản 1 Điều này.

Điều 3. Giải thích từ ngữ

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

1. *Mạng* được quy định tại Khoản 2 Điều 3 Luật An toàn thông tin mạng. Cụ thể: 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. *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.

3. *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.

4. *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.

5. *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.

6. *Rủi ro an toàn thông tin mạng* được quy định tại Khoản 8 Điều3 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.

7. *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.

8. *Nguy cơ mất an toàn thông tin mạng* là những nhân tố bên trong hoặc bên ngoài có khả năng ảnh hưởng tới trạng thái an toàn thông tin mạng.

9. *Tường lửa*: Là rào chắn được lập ra nhằm ngăn chặn người dùng mạng Internet truy cập thông tin không mong muốn hoặc (và) ngăn chặn người dùng từ bên ngoài truy cập các thông tin bảo mật nằm trong nội bộ, là một thiết bị phần cứng và (hoặc) phần mềm hoạt động trong môi trường mạng để ngăn chặn một số liên lạc bị cấm bởi chính sách an ninh của cá nhân hay tổ chức.

10. *Mạng truyền số liệu chuyên dùng* được quy định tại Khoản 1 Điều 3 Quyết định số 08/2023/QĐ-TTg ngày 05 tháng 4 năm 2023 của Thủ tướng Chính phủ về mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, nhà nước. Cụ thể: Mạng truyền số liệu chuyên dùng là mạng kết nối các cơ quan Đảng, Nhà nước, được tổ chức, quản lý thống nhất, bảo đảm chất lượng, an toàn, bảo mật thông tin để trao đổi, chia sẻ dữ liệu giữa các cơ quan Đảng, Nhà nước.

Điều 4. Nguyên tắc bảo đảm an toàn thông tin mạng

Bảo đảm an toàn thông tin mạng tuân thủ các nguyên tắc chung quy định tại Điều 4 Luật An toàn thông tin mạng và Điều 4 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 (*sau đây gọi tắt là Nghị định số 85/2016/NĐ-CP*).

Chương II
AN TOÀN THÔNG TIN MẠNG TRONG THIẾT KẾ, XÂY DỰNG, VẬN HÀNH HỆ THỐNG THÔNG TIN

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

1. Dự án đầu tư xây dựng mới hoặc mở rộng, nâng cấp hệ thống thông tin, chủ đầu tư xây dựng thuyết minh đề xuất cấp độ an toàn hệ thống thông tin theo Điều 13 Nghị định 85/2016/NĐ-CP.

2. Thiết kế, xây dựng các giải pháp bảo đảm an toàn thông tin phải tuân thủ nguyên tắc đồng bộ, có thể dùng chung, chia sẻ để tối ưu hiệu năng thiết bị và hiệu quả đầu tư.

3. Trước khi đưa vào vận hành, khai thác hệ thống thông tin: Chủ đầu tư 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 tháng 9 năm 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. Đồng thời, hệ thống thông tin phải được phê duyệt cấp độ an toàn hệ thống thông tin và triển khai đầy đủ phương án bảo đảm an toàn thông tin theo hồ sơ đề xuất cấp độ được phê duyệt.

Điều 6. An toàn thông tin mạng đối với thuê dịch vụ công nghệ thông tin

1. Khi ký kết hợp đồng thuê dịch vụ công nghệ thông tin, cơ quan chủ trì thuê dịch vụ phải xác định rõ phạm vi, trách nhiệm, quyền hạn và nghĩa vụ của các bên về bảo đảm an toàn thông tin mạng, điều kiện xử lý vi phạm quy định bảo đảm an toàn thông tin mạng 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 công nghệ thông tin, cơ quan chủ trì thuê dịch vụ có trách nhiệm:

a) Yêu cầu bên cung cấp dịch vụ phải bảo mật thông tin, dữ liệu, mã nguồn, tài liệu thiết kế hệ thống thông tin; triển khai các biện pháp bảo đảm an toàn thông tin mạng tuân thủ phương án bảo đảm an toàn thông tin được cấp có thẩm quyền phê duyệt, các quy định tại Quy chế này, Luật An toàn thông tin mạng và các quy định khác của pháp luật có liên quan.

b) Quản lý thông tin, dữ liệu phát sinh từ dịch vụ đã thuê; bảo đảm bên cung cấp dịch vụ không được truy cập để quản trị dữ liệu thuộc phạm vi nhà nước quản lý lưu trữ trên hệ thống thuê.

c) Giám sát, giới hạn quyền của bên cung cấp dịch vụ khi cho phép truy cập vào hệ thống thông tin để xử lý sự cố hoặc hỗ trợ nâng cấp, quản trị, vận hành.

3. Khi phát hiện bên cung cấp dịch vụ có dấu hiệu vi phạm quy định bảo đảm an toàn thông tin mạng, cơ quan chủ trì thuê dịch vụ có trách nhiệm:

a) Tạm dừng hoặc đình chỉ hoạt động của hệ thống thông tin tùy theo mức độ vi phạm và thông báo cho bên cung cấp dịch vụ.

b) Thu hồi quyền truy cập hệ thống thông tin đã cấp cho bên cung cấp dịch vụ (nếu có).

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

4. Kết thúc thời gian thuê dịch vụ, cơ quan chủ trì thuê dịch vụ có trách nhiệm:

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

b) Thu hồi và thay đổi mật khẩu hoặc hủy bỏ tài khoản truy cập hệ thống thông tin đã cấp cho bên cung cấp dịch vụ.

Điều 7. Quản lý an toàn hạ tầng mạng

1. An toàn cho mạng nội bộ

a) Phải sử dụng 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.

b) Khi kết nối từ xa vào mạng nội bộ, phải sử dụng giao thức mạng có mã hóa thông tin và thiết lập mật khẩu mạnh.

2. Mạng không dây để kết nối với mạng nội bộ phải thiết lập mật khẩu mạnh, mã hóa dữ liệu theo cơ chế bảo mật WPA2 hoặc WPA3. Mật khẩu truy cập phải được thay đổi định kỳ 06 tháng/lần.

3. Hệ điều hành, phần mềm tích hợp trên các thiết bị mạng phải thường xuyên được cập nhật các bản vá lỗi theo khuyến nghị của các nhà sản xuất.

4. Phải lưu trữ nhật ký khi thay đổi cấu hình kỹ thuật của các thiết bị mạng.

Điều 8. Quản lý an toàn máy chủ và ứng dụng

1. Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ

a) Máy chủ phải được cài đặt, sử dụng phần mềm phòng chống mã độc. Phần mềm phòng chống mã độc được cập nhật thường xuyên và phải có tính năng kỹ thuật đáp ứng yêu cầu của Bộ Thông tin và Truyền thông.

b) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn.

c) 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.

d) Thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng.

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

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

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

h) Bảo đảm các kết nối mạng trên máy chủ hoạt động liên tục, ổn định và an toàn. Cấu hình, kiểm soát các kết nối, các cổng dịch vụ từ bên trong đi ra, bên ngoài đi vào hệ thống.

2. Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống trước khi đưa vào vận hành, khai thác

a) Xây dựng, áp dụng quy trình cấu hình tối ưu, tăng cường bảo mật cho các máy chủ.

b) Máy chủ phải được rà soát, cấu hình tối ưu, tăng cường bảo mật trước khi đưa hệ thống vào vận hành khai thác.

3. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố

a) Triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

b) Phải thực hiện lưu trữ thay đổi cấu hình kỹ thuật của máy chủ, hệ điều hành, phần mềm.

4. Nghiêm cấm sử dụng các tài nguyên tính toán, gồm: 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 9. Bảo đảm an toàn thiết bị đầu cuối

1. Máy tính cá nhân phải đặt mật khẩu truy cập và chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng; thường xuyên cập nhật bản vá lỗ hổng bảo mật hệ điều hành và phần mềm ứng dụng; cài đặt phần mềm phòng chống mã độc và thiết

lập chế độ tự động cập nhật mẫu mã độc mới, tự động rà quét khi sao chép, mở các tập tin. Phần mềm phòng chống mã độc phải có tính năng kỹ thuật đáp ứng yêu cầu của Bộ Thông tin và Truyền thông.

2. Khi sử dụng máy tính, thiết bị đầu cuối trong mạng nội bộ cơ quan để xử lý công việc mang tính chất công vụ phải tuân thủ các quy định sau:

a) Không cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn trên máy tính của cơ quan.

b) Cán bộ, công chức, viên chức và người lao động phải tự đặt mật khẩu đăng nhập vào các hệ thống thông tin; thường xuyên thay đổi để tăng cường công tác bảo mật.

c) Không tự ý gỡ bỏ phần mềm phòng chống mã độc trên máy tính. Tất cả các tập tin, thư mục khi sao chép vào máy tính từ thiết bị ngoại vi phải được quét mã độc trước khi thực hiện.

d) Chỉ sử dụng thư điện tử công vụ để trao đổi, gửi, nhận tài liệu công vụ.

e) Khi phát hiện dấu hiệu máy tính nhiễm mã độc phải kịp thời thông báo cho bộ phận có trách nhiệm của cơ quan để xử lý.

3. Cá nhân khi mang máy tính, thiết bị di động thuộc sở hữu riêng kết nối với mạng nội bộ để xử lý công việc phải được sự đồng ý của thủ trưởng cơ quan và tuân thủ các quy định tại khoản 1 và khoản 2 Điều này.

Điều 10. Giám sát an toàn hệ thống thông tin

1. Hệ thống thông tin phải 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 đặt tại Trung tâm dữ liệu của tỉnh, Sở Thông tin và Truyền thông có trách nhiệm tổ chức giám sát an toàn thông tin theo quy định.

3. Đối với các hệ thống thông tin, phần mềm, ứng dụng, cơ sở dữ liệu không được đặt tại Trung tâm dữ liệu của tỉnh, đơn vị quản lý, vận hành có trách nhiệm tự thực hiện hoặc 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.

Điều 11. Kiểm tra, đánh giá an toàn hệ thống thông tin

Định kỳ tổ chức đánh giá, kiểm tra đối với hệ thống thông tin thuộc phạm vi quản lý của cơ quan, đơn vị mình theo quy định tại điểm c khoản 2 Điều 3 Nghị định số 85/2016/NĐ-CP. 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 12. Quản lý an toàn thông tin của các cơ quan, đơn vị đối với người sử dụng

1. Các cơ quan, đơn vị khi tiếp nhận, tuyển dụng 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. Các cơ quan, đơn vị 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. Các cơ quan, đơn vị có trách nhiệm quản lý và thu hồi tài khoản, quyền truy cập các hệ thống thông tin và tất cả các tài sản liên quan tới hệ thống thông tin khi cán bộ chuyển công tác, nghỉ việc, nghỉ theo chế độ.

Điều 13. Quản lý truy cập

1. Đối với cơ quan, đơn vị, người sử dụng

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 tincó 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 cơ quan, 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 14. Quản lý nhật ký trong quá trình vận hành các hệ thống thông tin

1. Các cơ quan, đơn vị phải thực hiện việc ghi nhật ký trên các thiết bị mạng máy tính, phần mềm ứng dụng, hệ điều hành, cơ sở dữ liệu nhằm bảo đảm các sự kiện quan trọng xảy ra trên hệ thống được ghi nhận và lưu giữ. Các bản ghi nhật ký này phải được bảo vệ an toàn nhằm sử dụng để phục vụ công tác kiểm tra, phân tích khi cần thiết.

2. Các sự kiện tối thiểu cần phải được ghi nhật ký gồm: quá trình đăng nhập hệ thống; tạo, cập nhật hoặc xóa dữ liệu; các hành vi xem, thiết lập cấu hình hệ thống; việc thiết lập các kết nối bất thường vào và ra hệ thống; thay đổi quyền truy cập hệ thống.

3. Thường xuyên thực hiện việc theo dõi bản ghi nhật ký của hệ thống và các sự kiện khác có liên quan để đánh giá, báo cáo các rủi ro và mức độ nghiêm trọng các rủi ro đó.

Điều 15. Phòng chống phần mềm độc hại

1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống phần mềm độc hại. Các phần mềm phòng chống phần mềm độc hại phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét phần mềm độc hại khi sao chép, mở các tập tin, có kết nối, chia sẻ thông tin với các hệ thống thông tin quản lý theo quy định hiện hành.

2. Hệ điều hành, phần mềm cài đặt trên máy chủ, máy trạm phải được cập nhật vá lỗ hổng bảo mật thường xuyên, kịp thời.

3. Cán bộ, công chức, viên chức và người lao động không được tự ý gỡ bỏ các phần mềm phòng, chống phần mềm độc hại trên máy tính khi chưa có sự đồng ý của người có thẩm quyền trong cơ quan.

4. Tất cả các máy tính của đơn vị phải được cấu hình vô hiệu hóa tính năng tự động thực thi (autoplay) các tập tin trên các thiết bị lưu trữ di động.

5. Các máy tính xách tay, thiết bị di động (*điện thoại thông minh, máy tính bảng...*) trước khi kết nối vào mạng LAN nội bộ của cơ quan, đơn vị phải bảo đảm đã được cài chương trình phòng chống phần mềm độc hại và đã được kiểm duyệt về các phần mềm độc hại.

6. Tất cả các tập tin, thư mục phải được quét phần mềm độc hại trước khi sao chép, sử dụng.

7. Máy chủ chỉ được dùng để cài đặt các phần mềm, dịch vụ dùng chung của cơ quan, đơn vị; không cài đặt phần mềm không rõ nguồn gốc, phần mềm phục vụ mục đích cá nhân và mục đích khác, không phục vụ công việc.

8. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy trạm như: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống phần mềm độc hại, tình trạng này lặp đi lặp lại nhiều lần, ở các vị trí khác nhau; quan trọng nhất là có dấu hiệu mất dữ liệu, người sử dụng phải tắt máy, ngắt kết nối từ máy tính đến mạng LAN nội bộ, mạng WAN nội tỉnh, mạng Internet và báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý.

Điều 16. Sao lưu dữ liệu dự phòng

1. Đối với các Cơ quan, đơn vị 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, bao gồm: cơ sở dữ liệu và 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 vẹnnhằm 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 cơ quan, 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.

Điều 17. Quản lý và ứng cứu sự cố an toàn thông tin

1. Phân loại mức độ nghiêm trọng của các sự cố, bao gồm:

a) Thấp: sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan, 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 1 (một) phòng, ban thuộc đơn vị bị ngưng hoạt động, phần mềm độc hại lây nhiễm tất cả các máy tính trạm trong 01 phòng, ban;

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, hồ sơ cấp phép, một cửa 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. 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:

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;

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;

Bước 3: Báo cáo sự cố đến Sở Thông tin và Truyền thông theo Mẫu số 03 ban hành kèm theo 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 (*sau đây gọi tắt là Thông tư số 20/2017/TT-BTTTT*) và thực hiện tiếp Bước 4;

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;

Bước 5: Lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố theo Mẫu số 04 ban hành kèm theo Thông tư số 20/2017/TT-BTTTT, 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.

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

4. Đường dây nóng hỗ trợ của Đội ứng cứu sự cố an toàn thông tin mạng chi tiết đăng tải trên Cổng thông tin điện tử Sở Thông tin và Truyền thông tại địa chỉ https://sotttt.haiduong.gov.vn/, chuyên mục Ứng cứu sự cố máy tính.

Chương III
TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 18. Trách nhiệm của Sở Thông tin và Truyền thông

1. Tham mưu giúp Ủy ban nhân dân tỉnh quản lý về công tác bảo đảm an toàn thông tin mạng trên địa bàn tỉnh và chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong việc tham mưu bảo đảm an toàn thông tin mạng cho các hệ thống thông tin của tỉnh.

2. Chỉ đạo, tổ chức bảo đảm an toàn thông tin mạng cho hạ tầng kỹ thuật của Trung tâm dữ liệu tỉnh.

3. Hằng 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 cơ quan nhà nước trên địa bàn tỉnh theo quy định.

4. Xây dựng và triển khai các chương trình đào tạo, tuyên truyền về an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh.

5. Định kỳ tổ chức diễn tập ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh, tham gia diễn tập quốc gia và quốc tế do Bộ Thông tin và Truyền thông tổ chức.

6. Chỉ đạo, hướng dẫn về nghiệp vụ về bảo đảm an toàn thông tin mạng; hỗ trợ giải quyết sự cố khi có yêu cầu.

7. Chủ trì, phối hợp với các cơ quan 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 trên địa bàn tỉnh.

8. Hướng dẫn, giám sát các cơ quan, đơn vị trên địa bàn tỉnh 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.

9. Tổng hợp và báo cáo về tình hình an toàn thông tin mạng theo định kỳ cho Bộ Thông tin và Truyền thông, Ủy ban nhân dân tỉnh và các cơ quan, đơn vị có liên quan.

Điều 19. Trách nhiệm của Công an tỉnh

1. Chủ trì, phối hợp với các sở, ngành có liên quan xây dựng và trình cấp có thẩm quyền ban hành và hướng dẫn thực hiện văn bản quy phạm pháp luật về bảo vệ bí mật nhà nước, phòng, chống tội phạm mạng, lợi dụng mạng để xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên địa bàn tỉnh.

2. Tổ chức, chỉ đạo, triển khai công tác phòng, chống tội phạm, tổ chức điều tra tội phạm mạng và hành vi vi phạm pháp luật khác trong lĩnh vực an toàn thông tin mạng.

3. Phối hợp với Sở Thông tin và Truyền thông và các sở, ngành có liên quan kiểm tra, thanh tra về an toàn thông tin mạng, xử lý vi phạm pháp luật về an toàn thông tin mạng theo thẩm quyền.

Điều 20. Trách nhiệm của Sở Kế hoạch và Đầu tư

Tổng hợp các Đề án, Dự án về bảo đảm an toàn thông tin mạng của các sở, ban, ngành; Chủ trì, phối hợp các đơn vị liên quan tham mưu UBND tỉnh trình Hội đồng nhân dân thông qua vốn phân bổ kế hoạch vốn trung hạn và hằng năm của các sở, ban, ngành thực hiện các Đề án, Dự án về bảo đảm an toàn thông tin mạng.

Điều 21. Trách nhiệm của Sở Tài chính

Hằng năm, căn cứ khả năng cân đối ngân sách và chế độ, tiêu chuẩn, định mức do nhà nước ban hành, tham mưu UBND tỉnh bố trí kinh phí triển khai thực hiện các dự án, nhiệm vụ về bảo đảm an toàn thông tin mạng.

Điều 22. Trách nhiệm của các cơ quan, đơn vị

1. Thủ trưởng cơ quan, đơn vị có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong công tác bảo đảm an toàn thông tin mạng của cơ quan, đơn vị mình.

2. Phân công bộ phận hoặc cán bộ chuyên trách 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.

3. Ban hành quy định, quy trình nội bộ về bảo đảm an toàn thông tin mạng phù hợp với Quy chế này và các quy định của pháp luật.

4. Các cơ quan, đơn vị có trách nhiệm thực hiện xác định cấp độ an toàn thông tin mạng và bảo đảm an toàn cho hệ thống thông tin của đơn vị quản lý theo quy định tại Luật An toàn thông tin mạng, Nghị định số 85/2016/NĐ-CP và hướng dẫn tại Thông tư 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 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.

5. 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.

6. 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.

Điều 23. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các cơ quan, đơn vị

1. Trách nhiệm của cán bộ, công chức, viên chức phụ trách an toàn thông tin mạng:

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 đảman 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.

2. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các cơ quan, đơn vị:

a) Nghiêm túc chấp hành các quy định, quy trình nội bộ, 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 toàn, an ninh thông tin đồng thời chịu trách nhiệm đối với các thông tin mà mình cung cấp. Mỗi cán bộ, công chức, viên 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 mang bí mật nhà nước lên hệ thống 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 thống thư điện tử tỉnh *(@haiduong.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, viên 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, bồi dưỡng về an toàn thông tin mạng do các cơ quan, đơn vị chuyên trách an toàn thông tin mạng hoặc Sở Thông tin và Truyền thông tổ chức.

Điều 24. Trách nhiệm của các tổ chức, cá nhân khác

Các tổ chức, cá nhân khác có sử dụng các hệ thống thông tin do ủy ban nhân dân tỉnh triển khai hoặc liên quan đến hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Hải Dương phải tuân thủ Quy chế này và các quy định hiện hành của pháp luật có liên quan.

Chương IV
ĐIỀU KHOẢN THI HÀNH

Điều 25. Tổ chức thực hiện

Sở Thông tin và Truyền thông chủ trì, phối hợp với các sở, ban, ngành, Ủy ban nhân dân các huyện, thị xã, thành phố và các tổ chức, cá nhân có liên quan triển khai thực hiện Quy chế này.

Thủ trưởng các sở, ban, ngành, đơn vị thuộc Ủy ban nhân dân tỉnh, Chủ tịch Ủy ban nhân dân các huyện, thị xã, thành phố chịu trách nhiệm tổ chức triển khai thực hiện Quy chế tại cơ quan, đơn vị, địa phương mình.

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