

Số: 455 /QĐ-SNNMT

Hưng Yên, ngày 26 tháng 9 năm 2025

QUYẾT ĐỊNH

**Ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng
Sở Nông nghiệp và Môi trường tỉnh Hưng Yên**

GIÁM ĐỐC SỞ NÔNG NGHIỆP VÀ MÔI TRƯỜNG TỈNH HƯNG YÊN

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13;

Căn cứ Luật An ninh mạng số 24/2018/QH14;

Căn cứ Nghị định số 47/2020/NĐ-CP của Chính phủ quy định về quản lý, kết nối và chia sẻ dữ liệu số của cơ quan nhà nước;

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 Nghị định số 53/2022/NĐ-CP ngày 15 tháng 8 năm 2022 của Chính phủ về quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Nghị định số 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 của Chính phủ về bảo vệ dữ liệu cá nhân;

Căn cứ Nghị định số 147/2024/NĐ-CP ngày 09 tháng 11 năm 2024 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 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 01/7/2016 của Chính phủ về bảo đảm an toàn HTTT theo cấp độ;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ 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 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;

Căn cứ các Quyết định số 06/2025/QĐ-UBND ngày 01/07/2025 của Ủy ban nhân dân tỉnh Hưng Yên về việc Quy định chức năng, nhiệm vụ, quyền hạn, cơ cấu tổ chức của Sở nông nghiệp và môi trường tỉnh Hưng Yên;

Theo đề nghị của Chánh Văn phòng Sở.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Sở Nông nghiệp và Môi trường tỉnh Hưng Yên.

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

Điều 3. Chánh Văn phòng Sở; Trưởng các phòng, đơn vị; toàn thể cán bộ, công chức, viên chức, người lao động thuộc các phòng, đơn vị trực thuộc Sở Nông nghiệp và Môi trường tỉnh Hưng Yên chịu trách nhiệm thi hành Quyết định này. / *le*

Nơi nhận:

- Như điều 3;
- Công an tỉnh (để t/d);
- Lãnh đạo sở;
- Lưu: VT, VP.



GIÁM ĐỐC

Nguyễn Đức Kiên
Nguyễn Đức Kiên

QUY CHẾ

Bảo đảm an toàn thông tin mạng, an ninh mạng Sở Nông nghiệp và Môi trường tỉnh Hưng Yên

(Kèm theo Quyết định số /QĐ-SNNMT ngày / /2025 của Sở Nông
nghiệp và Môi trường tỉnh Hưng Yên)

Chương I. QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh

Quy chế này quy định về bảo đảm an toàn thông tin mạng và an ninh mạng trong các hoạt động chuyển đổi số, ứng dụng công nghệ thông tin, vận hành, khai thác hệ thống, hạ tầng thông tin, phần mềm, dữ liệu thuộc phạm vi quản lý của Sở Nông nghiệp và Môi trường tỉnh Hưng Yên.

2. Đối tượng áp dụng

a) Các phòng, đơn vị thuộc và trực thuộc Sở Nông nghiệp và Môi trường tỉnh Hưng Yên; các cán bộ, công chức, viên chức và người lao động tại các phòng, đơn vị thuộc và trực thuộc Sở Nông nghiệp và Môi trường tỉnh Hưng Yên và các đối tượng tham gia vận hành, khai thác các hệ thống thông tin (HTTT) của Sở Nông nghiệp và Môi trường tỉnh Hưng Yên.

b) Cơ quan, tổ chức, cá nhân có kết nối, sử dụng các HTTT của Sở Nông nghiệp và Môi trường tỉnh Hưng Yên.

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ quản lý, vận hành, duy trì, phát triển và bảo đảm an toàn thông tin mạng phục vụ hoạt động cho các HTTT của Sở Nông nghiệp và Môi trường tỉnh Hưng Yên.

Điều 2. Giải thích từ ngữ

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

1. *An toàn thông tin mạng* là sự bảo vệ thông tin, HTTT 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. *An ninh mạng* là việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

3. *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.

4. *Hạ tầng kỹ thuật* là tập hợp các thiết bị tính toán, lưu trữ, thiết bị ngoại vi, thiết bị kết nối mạng, thiết bị phụ trợ, đường truyền, mạng nội bộ, mạng diện rộng...

5. *Chủ quản HTTT* là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với HTTT.

7. *Sự cố an toàn thông tin mạng* là việc thông tin, HTTT bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

8. *Mạng* là một hệ thống kết nối nhiều thiết bị với nhau (như máy tính, điện thoại, máy in, máy chủ...) nhằm mục đích chia sẻ dữ liệu, tài nguyên và thông tin.

9 *Người dùng* là cán bộ, công chức, viên chức, người lao động tại các phòng, đơn vị thuộc Sở sử dụng thiết bị số để xử lý công việc.

10. *Phần mềm độc hại* là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ HTTT hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong HTTT.

11. *Thiết bị số* là thiết bị điện tử, máy tính, viễn thông, truyền dẫn, thu phát sóng vô tuyến điện và thiết bị tích hợp khác được sử dụng để sản xuất, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin số.

Điều 3. Nguyên tắc bảo đảm an toàn, an ninh thông tin mạng

1. Bảo đảm an toàn, an ninh thông tin là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt quá trình liên quan đến thông tin và thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ HTTT. Bảo đảm an toàn, an ninh thông tin 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 và các quy định pháp luật khác có liên quan.

2. Tuân thủ các quy định và hướng dẫn về bảo đảm an toàn, an ninh thông tin của cơ quan có thẩm quyền. Trường hợp có văn bản, quy định cập nhật, thay thế hoặc quy định khác tại văn bản quy phạm pháp luật, quyết định của cấp có thẩm quyền cao hơn thì áp dụng quy định tại văn bản đó.

3. Trách nhiệm bảo đảm an toàn thông tin mạng và an ninh mạng gắn với trách nhiệm của người đứng đầu các phòng, đơn vị và cá nhân trực tiếp liên quan.

4. Việc bảo đảm an toàn HTTT được thực hiện một cách tổng thể, đồng bộ, tập trung trong việc đầu tư các giải pháp bảo vệ, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp.

5. Quản lý, sử dụng và bảo đảm an ninh mạng, mạng máy tính nội bộ có lưu trữ, truyền đưa bí mật nhà nước phải được tách biệt vật lý hoàn toàn với mạng máy tính, các thiết bị, phương tiện điện tử có kết nối mạng Internet, trường hợp khác phải bảo đảm quy định của pháp luật về bảo vệ bí mật nhà nước.

6. Xử lý sự cố an toàn thông tin phải phù hợp với trách nhiệm, quyền hạn và bảo đảm lợi ích hợp pháp của phòng, đơn vị, cá nhân liên quan và theo quy định của pháp luật.

7. Các HTTT, cơ sở dữ liệu của Sở và các đơn vị trực thuộc phải được phê duyệt hồ sơ đề xuất cấp độ và có phương án bảo đảm an toàn thông tin tương ứng với cấp độ trước khi đưa vào sử dụng.

8. Mỗi công chức, viên chức, người lao động tại các phòng, đơn vị nêu cao tinh thần chủ động, tự giác trong việc áp dụng các biện pháp bảo đảm an toàn, an ninh mạng.

Điều 4. Các hành vi bị nghiêm cấm

1. Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật An toàn thông tin mạng, Điều 8 Luật An ninh mạng và Điều 5 Luật Bảo vệ bí mật nhà nước.

2. Tự ý đầu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập mạng không dây của cá nhân vào mạng nội bộ; tự ý thay đổi, gỡ bỏ biện 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.

3. Tiết lộ thiết kế, thông số cấu hình hệ thống cho tổ chức, cá nhân khác khi không được phép; tìm cách truy cập dưới bất cứ hình thức nào vào các khu vực không được phép truy cập.

4. Sử dụng hạ tầng, trang thiết bị công nghệ thông tin của phòng, đơn vị để đào tiền ảo, đánh bạc, cá độ.

5. Phát tán thư rác, phần mềm độc hại, thiết lập HTTT giả mạo, lừa đảo.

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

7. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

8. Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của HTTT hoặc tới khả năng truy cập HTTT của người sử dụng.

9. Các hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

Chương II

QUY ĐỊNH BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG, AN NINH MẠNG

Điều 5. Phân công thực hiện vai trò về bảo đảm an toàn thông tin mạng cho các HTTT theo quy định của pháp luật

1. Phòng, đơn vị vận hành HTTT:

a) Đơn vị vận hành HTTT được xác định theo Khoản 1, Khoản 2 Điều 5 Thông tư số 12/2022/TT-BTTTT;

b) Trường hợp thuê dịch vụ công nghệ thông tin, đơn vị vận hành được xác định theo Khoản 3 Điều 5 Thông tư số 12/2022/TT-BTTTT.

2. Đơn vị phụ trách về an toàn thông tin:

a) Văn phòng Sở là đơn vị phụ trách an toàn thông tin của Sở Nông nghiệp và Môi trường.

b) Phòng phụ trách công nghệ thông tin, chuyên đổi số các đơn vị trực thuộc Sở là đơn vị phụ trách về an toàn thông tin.

Điều 6. Trình tự, thủ tục, thẩm quyền xác định cấp độ HTTT

1. Đơn vị lập hồ sơ đề xuất cấp độ

Đối với các HTTT thuộc các nhiệm vụ, dự án đang trong giai đoạn lập dự án, đơn vị lập dự án lập hồ sơ đề xuất cấp độ. Đối với các HTTT đang triển khai và vận hành, đơn vị vận hành lập hồ sơ đề xuất cấp độ.

2. Nội dung của hồ sơ đề xuất cấp độ HTTT quy định tại Điều 15 Nghị định số 85/2016/NĐ-CP và Điều 8, Điều 9 Thông tư số 12/2022/TT-BTTTT.

3. Nội dung, thời gian thẩm định hồ sơ đề xuất cấp độ HTTT quy định tại Điều 16 Nghị định số 85/2016/NĐ-CP.

4. Thẩm quyền, trình tự, thủ tục xác định cấp độ HTTT quy định tại Điều 12, Điều 13, Điều 14 Nghị định số 85/2016/NĐ-CP và Điều 6 Thông tư số 12/2022/TT-BTTTT.

Điều 7. Phương án bảo đảm an toàn HTTT

1. Phương án bảo đảm an toàn HTTT đối với từng cấp độ phải đáp ứng yêu cầu quy định tại Điều 10 Thông tư số 12/2022/TT-BTTTT.

2. Phòng, đơn vị quản lý trực tiếp HTTT tổ chức triển khai phương án bảo đảm an toàn HTTT sau khi hồ sơ đề xuất cấp độ hoặc phương án bảo đảm an toàn hệ thống được phê duyệt.

3. Bộ phận phụ trách về an toàn thông tin thuộc đơn vị chịu trách nhiệm giám sát việc triển khai các phương án bảo đảm an toàn thông tin đã được phê duyệt.

4. Đơn vị vận hành phải xây dựng Quy chế bảo đảm an toàn, an ninh mạng cho HTTT đáp ứng các yêu cầu về quản lý theo cấp độ an toàn HTTT tương ứng; có thể ban hành độc lập hoặc lồng ghép vào Quy chế quản lý, duy trì, vận hành, sử dụng HTTT; và được cấp có thẩm quyền phê duyệt, ban hành trước khi Hồ sơ đề xuất cấp độ được phê duyệt.

Điều 8. Quản lý an toàn, an ninh thông tin khi tiếp nhận, phát triển, vận hành và bảo trì HTTT

1. Khi thực hiện nâng cấp, mở rộng, thay thế một phần HTTT, phải rà soát cấp độ, phương án bảo đảm an toàn của HTTT và thực hiện điều chỉnh, bổ sung hoặc thay mới hồ sơ đề xuất cấp độ trong trường hợp cần thiết.

2. Khi tiếp nhận, phát triển, nâng cấp, bảo trì HTTT, phòng, đơn vị phải tiến hành phân tích, xác định rủi ro có thể xảy ra, đánh giá phạm vi tác động và phải chuẩn bị các biện pháp hạn chế, loại trừ các rủi ro này và yêu cầu các bên cung cấp, thi công, các cá nhân liên quan thực hiện.

Điều 9. Quản lý an toàn, an ninh thông tin đối với hạ tầng mạng, hệ thống máy chủ và thiết bị số

1. Hạ tầng mạng

a) Hệ thống mạng nội bộ

- Phải được thiết kế phân vùng theo chức năng cơ bản (theo các chính sách an toàn thông tin riêng), bao gồm: vùng mạng người dùng; vùng mạng kết nối hệ thống ra bên ngoài Internet và các mạng khác; vùng mạng máy chủ công cộng; vùng mạng máy chủ nội bộ; vùng mạng máy chủ quản trị;

- Dữ liệu trao đổi giữa các vùng mạng phải được quản lý, giám sát bởi hệ thống các thiết bị bảo mật và giám sát an toàn, an ninh thông tin;

- Thiết lập, cấu hình các tính năng theo thiết kế của các trang thiết bị bảo mật mạng; thực hiện các biện pháp, giải pháp để dò tìm và phát hiện kịp thời các

điểm yếu, lỗ hổng về mặt kỹ thuật của hệ thống mạng; thường xuyên kiểm tra, phát hiện những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào mạng;

- Định kỳ sao lưu cấu hình thiết bị kết nối mạng nội bộ. Lưu trữ tối thiểu trong 03 tháng đối với nhật ký của các thiết bị mạng và bảo đảm đồng bộ thời gian nhật ký với máy chủ thời gian thực theo múi giờ Việt Nam;

- Các đường truyền dữ liệu, đường truyền Internet và các hệ thống dây cáp mạng phải được lắp đặt trong ống, máng che đậy kín, hạn chế khả năng tiếp cận trái phép. Ngắt kết nối các công mạng không sử dụng;

- Không được tiết lộ thiết kế, thông số cấu hình hệ thống mạng nội bộ cho tổ chức, cá nhân khác khi không được phép; không được tìm cách truy cập dưới bất cứ hình thức nào vào các khu vực không được phép truy cập.

b) Kết nối mạng Internet

Các đơn vị áp dụng các biện pháp kỹ thuật cần thiết bảo đảm an toàn thông tin trong kết nối vào Internet, tối thiểu đáp ứng các yêu cầu sau:

- Có hệ thống tường lửa và hệ thống bảo vệ truy cập Internet, đáp ứng nhu cầu kết nối đồng thời, hỗ trợ các công nghệ mạng riêng ảo thông dụng và có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ;

- Loại bỏ, không cho phép truy cập các trang tin có nghi ngờ chứa mã độc; hoạt động đánh bạc, lừa đảo trực tuyến; tuyên truyền phản động hoặc các nội dung không phù hợp khác.

c) Các đơn vị và cá nhân tham gia vào hệ thống mạng máy tính không được tự ý thay đổi thông số mạng hay tự ý đưa các thiết bị mạng, thiết bị viễn thông khác tham gia kết nối vào hệ thống mạng.

2. Hệ thống máy chủ

a) Phải được đặt trong các vùng mạng dành riêng cho máy chủ, tối thiểu gồm vùng mạng máy chủ công cộng, vùng mạng máy chủ nội bộ và vùng mạng máy chủ quản trị;

b) Chỉ cho phép kết nối đến những dịch vụ cần thiết trên Internet;

c) Chỉ mở và cung cấp các dịch vụ cần thiết ra Internet;

d) Chỉ cài đặt và sử dụng các phần mềm đúng bản quyền, nguồn gốc rõ ràng, thực sự cần thiết. Không sử dụng các phần mềm đã được cảnh báo không an toàn hoặc không được nhà sản xuất hỗ trợ kỹ thuật khi không thực sự cần thiết;

đ) Cài đặt các giải pháp phòng chống mã độc tập trung và phòng chống tấn công xâm nhập mạng phù hợp với yêu cầu theo từng cấp độ;

e) Triển khai các biện pháp sao lưu dự phòng để nâng cao khả năng phục hồi hoạt động khi xảy ra sự cố;

g) Giám sát thường xuyên, liên tục để phát hiện và cảnh báo sớm nguy cơ mất an toàn thông tin.

3. Thiết bị số

a) Người sử dụng chỉ cài đặt phần mềm có hỗ trợ cập nhật các bản vá, tính năng mới, bản vá lỗ hổng bảo mật; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của bộ phận phụ trách về công nghệ thông tin;

thường xuyên cập nhật bản vá cho các phần mềm ứng dụng, hệ điều hành và các phần mềm phục vụ công việc;

b) Cài đặt phần mềm phòng, chống mã độc và phải thiết lập chế độ tự động cập nhật tính năng mới cho phần mềm khi có thông báo từ hãng khuyến nghị; khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính phải tắt máy và báo trực tiếp cho bộ phận phụ trách, phụ trách về công nghệ thông tin để được xử lý kịp thời;

c) Chỉ truy cập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; có trách nhiệm bảo mật tài khoản truy cập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác;

d) Khóa màn hình máy tính khi rời khỏi bàn làm việc. Đăng xuất khỏi hệ thống, ứng dụng khi ngừng sử dụng. Tắt máy an toàn sau mỗi buổi làm việc;

đ) Chỉ sử dụng thiết bị lưu trữ di động cho các hoạt động nghiệp vụ, quản lý khi được sự đồng ý của Lãnh đạo đơn vị; thực hiện các biện pháp bảo đảm an ninh, an toàn cho thiết bị lưu trữ di động như mã hóa dữ liệu, quét mã độc định kỳ;

e) Báo cáo và phải được người có thẩm quyền đồng ý, cho phép trước khi mang thiết bị số thuộc sở hữu riêng đến nơi làm việc và kết nối với mạng nội bộ để xử lý công việc;

g) Đối với thiết bị số phục vụ quản trị hệ thống: Chỉ được sử dụng cho mục đích quản trị hệ thống; chỉ cài đặt và sử dụng các phần mềm quản trị đúng bản quyền, nguồn gốc rõ ràng, thực sự cần thiết; không được kết nối trực tiếp đến máy chủ để thực hiện quản trị cấu hình mà phải kết nối với máy chủ quản trị qua các đường truyền có mã hóa bảo mật theo quy định.

Điều 10. Quản lý an toàn, an ninh thông tin đối với tài khoản truy cập

1. Người sử dụng truy cập vào các HTTT được cấp và sử dụng tài khoản truy cập với định danh duy nhất gắn với cá nhân đó. Các HTTT dùng chung sử dụng cơ chế đăng nhập một lần, chung một tài khoản truy cập và mật khẩu.

2. Trường hợp người sử dụng thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu, trong vòng không quá 05 ngày làm việc (từ thời điểm có quyết định chính thức) đơn vị quản lý cá nhân đó phải thông báo cho đơn vị chủ quản HTTT để điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng đối với HTTT; trường hợp HTTT có quy định phân cấp quyền quản trị để khóa, thu hồi, xóa quyền sử dụng khi cá nhân đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu thì không phải thông báo về đơn vị chủ quản HTTT.

3. Tài khoản quản trị hệ thống (mạng, hệ điều hành, thiết bị kết nối mạng, phần mềm, ứng dụng, cơ sở dữ liệu) phải tách biệt với tài khoản truy cập của người sử dụng thông thường. Tài khoản hệ thống phải được giao đích danh cá nhân làm công tác quản trị. Hạn chế dùng chung tài khoản quản trị.

4. Khi có yêu cầu khóa quyền truy cập HTTT của tài khoản đang hoạt động, lãnh đạo đơn vị phải yêu cầu bằng văn bản gửi đơn vị chủ quản HTTT. Đơn vị vận hành HTTT thực hiện việc khóa quyền truy cập của tài khoản khi có chỉ đạo của đơn vị chủ quản HTTT. Đơn vị chủ quản HTTT có quyền khóa

quyền truy cập của tài khoản trong trường hợp tài khoản đó thực hiện các hành vi tấn công hoặc dễ xảy ra vấn đề mất an toàn, an ninh thông tin.

5. Quy định về đặt mật khẩu cho tài khoản truy cập của người sử dụng: Việc đặt mật khẩu truy cập, sử dụng, quản trị HTTT; truy cập thiết bị lưu khóa bí mật và các tài khoản liên quan phục vụ công việc phải bảo đảm quy tắc:

a) Có tối thiểu 10 ký tự đối với tài khoản người dùng, tối thiểu 12 ký tự đối với tài khoản quản trị hệ thống; gồm tối thiểu 3 trong 4 loại ký tự sau: chữ cái viết hoa (A - Z); chữ cái viết thường (a - z); chữ số (0 - 9); các ký tự đặc biệt trên bàn phím máy tính (' ~ ! @ # \$ % ^ & * () _ - + = { } [] \ | : ; ' " ' < > , . ? /) và dấu cách. Mật khẩu không được chứa tên tài khoản;

b) Mật khẩu phải được đổi ngay sau khi nhận bàn giao từ người khác hoặc có thông báo về dấu hiệu tấn công mạng, sự cố an toàn thông tin, điểm yếu liên quan đến khả năng lộ mật khẩu; mật khẩu phải được đổi tối thiểu 12 tháng/lần đối với tài khoản người dùng, tối thiểu 02 tháng/lần đối với tài khoản quản trị;

c) Phải kích hoạt bảo mật nâng cao cho các tài khoản quản trị trên các hệ thống có hỗ trợ xác thực đa lớp;

d) Người sử dụng, người làm công tác quản trị hệ thống có trách nhiệm bảo vệ thông tin tài khoản được cấp, không tiết lộ mật khẩu hoặc đưa cho người khác phương tiện xác thực tài khoản của mình ngoại trừ các trường hợp: cần xử lý công việc khẩn cấp của đơn vị; cần cung cấp, bàn giao cho đơn vị các thông tin tài khoản do cá nhân quản lý.

Điều 11. Quản lý an toàn, an ninh thông tin đối với ứng dụng

1. Yêu cầu về bảo đảm an toàn thông tin phải được đưa vào tất cả các công đoạn thiết kế, xây dựng, triển khai và vận hành, sử dụng phần mềm, ứng dụng.

2. Phần mềm, ứng dụng phải đáp ứng các yêu cầu sau: cấu hình phần mềm, ứng dụng để xác thực người sử dụng; giới hạn số lần đăng nhập sai liên tiếp; giới hạn thời gian để chờ đóng phiên kết nối; mã hóa thông tin xác thực trên hệ thống; không khuyến khích việc đăng nhập tự động.

3. Thiết lập, phân quyền truy cập, quản trị, sử dụng tài nguyên khác nhau của phần mềm, ứng dụng với người sử dụng/nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau; tách biệt cổng giao tiếp quản trị phần mềm ứng dụng với cổng giao tiếp cung cấp dịch vụ; đóng các cổng giao tiếp không sử dụng.

4. Chỉ cho phép sử dụng các giao thức mạng có hỗ trợ chức năng mã hóa thông tin như SSH, SSL, VPN hoặc tương đương khi truy cập, quản trị phần mềm, ứng dụng từ xa trên môi trường mạng; hạn chế truy cập đến mã nguồn của phần mềm, ứng dụng và phải đặt mã nguồn trong môi trường an toàn do bộ phận phụ trách công nghệ thông tin quản lý.

5. Ghi và lưu giữ bản ghi nhật ký hệ thống (log files) của phần mềm, ứng dụng trong khoảng thời gian tối thiểu 03 tháng với những thông tin cơ bản: thời gian, địa chỉ, tài khoản (nếu có), nội dung truy cập và sử dụng phần mềm, ứng dụng; các lỗi phát sinh trong quá trình hoạt động; thông tin đăng nhập khi quản trị.

6. Phần mềm, ứng dụng cần kiểm tra phát hiện và khắc phục các điểm yếu về an toàn, an ninh thông tin trước khi đưa vào sử dụng và trong quá trình sử dụng.

7. Thực hiện quy trình kiểm soát cài đặt, cập nhật, vá lỗi bảo mật phần mềm, ứng dụng trên các máy chủ, máy tính cá nhân, thiết bị kết nối mạng đang hoạt động thuộc hệ thống mạng nội bộ.

Điều 12. Quản lý an toàn, an ninh thông tin đối với dữ liệu

1. Các phòng, đơn vị phải thực hiện bảo vệ thông tin, dữ liệu liên quan đến hoạt động công vụ, thông tin có nội dung quan trọng, nhạy cảm hoặc không phải là thông tin công khai bằng các biện pháp như: thiết lập phương án bảo đảm tính bí mật, nguyên vẹn và khả dụng của thông tin, dữ liệu; mã hóa thông tin, dữ liệu khi lưu trữ trên hệ thống/thiết bị lưu trữ dữ liệu; sử dụng chữ ký số để xác thực và bảo mật thông tin, dữ liệu.

2. Các phòng, đơn vị cần 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.

3. Trang thiết bị công nghệ thông tin có lưu trữ dữ liệu nhạy cảm khi thay đổi mục đích sử dụng hoặc thanh lý, đơn vị phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó đảm bảo không có khả năng phục hồi. Trường hợp không thể tiêu hủy được dữ liệu, phòng, đơn vị phải thực hiện tiêu hủy cấu phần lưu trữ dữ liệu trên trang thiết bị công nghệ thông tin đó.

4. Trang thiết bị công nghệ thông tin có bộ phận lưu trữ hoặc thiết bị lưu trữ khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài hoặc ngừng sử dụng phải tháo bộ phận lưu trữ khỏi thiết bị hoặc xóa thông tin, dữ liệu lưu trữ trên thiết bị (trừ trường hợp để khôi phục dữ liệu). Khi thanh lý thiết bị phải xóa nội dung dữ liệu lưu trữ bằng phần mềm, thiết bị hủy dữ liệu chuyên dụng hoặc phá hủy vật lý.

5. Bố trí máy tính riêng không kết nối mạng, đặt mật khẩu và các biện pháp bảo mật phù hợp để soạn thảo, lưu trữ thông tin, tài liệu mật. Đối với các thiết bị chứa thông tin mật bắt buộc phải kết nối mạng thì phải áp dụng các giải pháp bảo mật an toàn, an ninh thông tin được Ban Cơ yếu Chính phủ đánh giá và cho phép.

6. Các phòng, đơn vị phải thường xuyên kiểm tra, giám sát các hoạt động chia sẻ, gửi, nhận thông tin, dữ liệu trong hoạt động nội bộ của mình; khuyến cáo việc chia sẻ, gửi, nhận thông tin trên môi trường mạng cần phải sử dụng mật khẩu để bảo vệ thông tin.

7. Đối với hoạt động trao đổi thông tin, dữ liệu với bên ngoài, đơn vị và cá nhân thực hiện trao đổi thông tin, dữ liệu ra bên ngoài cam kết và có biện pháp bảo mật thông tin, dữ liệu được trao đổi. Trường hợp dữ liệu trao đổi là dữ liệu cá nhân cần tuân thủ Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 về bảo vệ dữ liệu cá nhân. Giao dịch trực tuyến phải được truyền đầy đủ, đúng địa chỉ, tránh bị sửa đổi, tiết lộ hoặc nhân bản một cách trái phép; sử dụng các cơ chế xác thực mạnh, chữ ký số khi tham gia giao dịch, sử dụng các giao thức truyền thông an toàn.

Điều 13. Quản lý an toàn, an ninh thông tin đối với công chức, viên chức và người lao động

1. Điều kiện, yêu cầu của nhân sự làm công tác quản trị mạng, vận hành hệ thống, bảo đảm an toàn, an ninh mạng

a) Có phẩm chất đạo đức tốt, có đủ tiêu chuẩn chính trị, có kiến thức pháp luật và chuyên môn, nghiệp vụ về bảo vệ thông tin bí mật, nghiêm chỉnh chấp hành đường lối, chủ trương, chính sách của Đảng, pháp luật của Nhà nước;

b) Có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng.

2. Quy định trách nhiệm bảo đảm an toàn, an ninh thông tin trong quản lý và sử dụng nhân sự

a) Xác định các yêu cầu và trách nhiệm cụ thể của bộ phận, công chức, viên chức trong việc bảo đảm an toàn, an ninh thông tin cho từng vị trí phân công;

b) Phổ biến cho nhân sự mới tuyển dụng các quy định về bảo đảm an toàn, an ninh thông tin tại đơn vị. Định kỳ tổ chức quán triệt các quy định về an toàn, an ninh thông tin, nhằm nâng cao nhận thức về trách nhiệm bảo đảm an toàn, an ninh thông tin của từng cá nhân trong đơn vị;

c) Đối với các vị trí tiếp xúc, quản lý các thông tin, dữ liệu quan trọng hoặc quản trị các HTTT quan trọng, đơn vị phải yêu cầu công chức, viên chức mới cam kết bảo mật thông tin bằng văn bản hoặc cam kết trong hợp đồng làm việc, hợp đồng lao động, bao gồm các điều khoản về trách nhiệm của cá nhân sau khi thôi việc tại đơn vị;

d) Có biện pháp quản lý tài khoản người dùng của công chức, viên chức và người lao động trên các HTTT quan trọng;

đ) Thực hiện đúng quy trình cấp mới, quản lý và thu hồi tài khoản, phân quyền truy cập các HTTT và tất cả các tài sản liên quan đến HTTT đối với các cá nhân do phòng, đơn vị quản lý. Thường xuyên rà soát, kiểm tra quyền truy cập vào các HTTT đối với tất cả công chức, viên chức và người lao động bảo đảm quyền truy cập phù hợp với nhiệm vụ được giao.

3. Khi công chức, viên chức và người lao động quản lý an toàn, an ninh thông tin chấm dứt hoặc thay đổi công việc, các đơn vị phải:

a) Xác định rõ trách nhiệm của công chức, viên chức, người lao động và các bên liên quan trong quản lý, sử dụng tài sản công nghệ thông tin được giao;

b) Lập biên bản bàn giao tài sản công nghệ thông tin với đơn vị chủ quản và các đơn vị liên quan;

c) Thay đổi hoặc thu hồi quyền truy cập các HTTT;

d) Rà soát, kiểm tra đối chiếu định kỳ giữa bộ phận quản lý nhân sự và bộ phận quản lý cấp phát, thu hồi quyền truy cập HTTT để bảo đảm tài khoản người dùng của công chức, viên chức và người lao động đã nghỉ việc được thu hồi.

Điều 14. Giám sát an toàn thông tin mạng

1. Các HTTT phải được thực hiện giám sát an toàn thông tin.

2. Các HTTT bắt buộc phải có chức năng ghi và lưu trữ nhật ký về hoạt động của hệ thống và người sử dụng HTTT. Thực hiện việc bảo vệ các chức

năng ghi nhật ký và thông tin nhật ký, chống giả mạo, sửa đổi, phá hủy và truy cập trái phép.

3. Nguyên tắc, yêu cầu, nội dung, phương thức, hệ thống kỹ thuật phục vụ công tác giám sát thực hiện theo quy định tại Thông tư số 31/2017/TT-BTTTT.

4. Các đơn vị trực thuộc cử 01 lãnh đạo đơn vị và 01 cán bộ phụ trách an toàn thông tin làm đầu mối giám sát an toàn thông tin mạng để tiếp nhận cảnh báo, cung cấp, trao đổi, chia sẻ thông tin với cơ quan có thẩm quyền trong các hoạt động giám sát an toàn thông tin của đơn vị.

Điều 15. Kiểm tra, đánh giá an toàn thông tin mạng

1. Các HTTT phải được kiểm tra, đánh giá an toàn thông tin sau khi xây dựng, nâng cấp, mở rộng hệ thống hoặc định kỳ theo quy định đối với từng cấp độ.

2. Chủ quản HTTT có thẩm quyền yêu cầu kiểm tra, đánh giá an toàn, an ninh thông tin đối với các HTTT thuộc thẩm quyền quản lý. Đơn vị chuyên trách về an toàn, an ninh thông tin của chủ quản HTTT có thẩm quyền yêu cầu kiểm tra, đánh giá đối với các HTTT do đơn vị này phê duyệt hồ sơ đề xuất cấp độ.

3. 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 việc kiểm tra, đánh giá. Đối tượng kiểm tra, đánh giá là chủ quản HTTT hoặc đơn vị vận hành HTTT và các HTTT có liên quan.

4. Nội dung, hình thức kiểm tra, đánh giá theo quy định tại Điều 11 và Điều 12 Thông tư số 12/2022/TT-BTTTT.

Điều 16. Ứng cứu sự cố an toàn thông tin mạng

1. Đơn vị thường trực ứng cứu sự cố an toàn thông tin mạng của Sở:

a) Văn phòng Sở là đơn vị thường trực Đội ứng cứu sự cố an toàn thông tin mạng của Sở; rà soát trình Sở kiện toàn Đội ứng cứu an toàn thông tin mạng của Sở và tổ chức ứng cứu sự cố trong phạm vi của Sở quản lý.

b) Các đơn vị trực thuộc Sở rà soát, cử cán bộ phụ trách tham gia Đội ứng cứu sự cố an toàn thông tin mạng của Sở theo đề nghị của Văn phòng.

2. Kế hoạch ứng phó sự cố an toàn thông tin mạng của Sở:

a) Các đơn vị tổ chức xây dựng, phê duyệt kế hoạch ứng phó sự cố cho các HTTT do đơn vị trực tiếp quản lý theo đề cương tại Phụ lục II của Quyết định số 05/2017/QĐ-TTg và tổ chức triển khai kế hoạch sau khi phê duyệt.

b) Kế hoạch ứng phó sự cố được rà soát và điều chỉnh hàng năm (nếu cần thiết) trước ngày 31 tháng 10, làm cơ sở để xây dựng kế hoạch bảo đảm an toàn, an ninh thông tin năm tiếp theo.

3. Quy trình ứng cứu sự cố an toàn thông tin mạng của Sở:

a) Các phòng, đơn vị, tổ chức, cá nhân khi phát hiện dấu hiệu tấn công hoặc sự cố an toàn thông tin mạng cần nhanh chóng báo cho đơn vị vận hành HTTT, đơn vị chủ quản HTTT, Sở (qua Văn phòng).

b) Khi xảy ra sự cố an toàn thông tin mạng thuộc loại hình tấn công mạng, đơn vị vận hành HTTT thực hiện báo cáo theo quy định tại Điểm a Khoản 1 Điều 11 Quyết định số 05/2017/QĐ-TTg và Điều 9 Thông tư số 20/2017/TT-BTTTT, đồng thời báo cáo Sở (qua Văn phòng) để tổng hợp, báo cáo Lãnh đạo Sở. Trách nhiệm của các phòng, đơn vị khi phát hiện, tiếp nhận xác minh, xử lý

ban đầu và phân loại sự cố an toàn thông tin mạng theo quy định tại Điều 12 Quyết định số 05/2017/QĐ-TTg và Điều 10 Thông tư số 20/2017/TT-BTTTT;

c) Quy trình ứng cứu sự cố an toàn thông tin mạng quy định tại Điều 13, Điều 14 Quyết định số 05/2017/QĐ-TTg và Điều 11 Thông tư số 20/2017/TT-BTTTT.

Điều 17. Đào tạo, bồi dưỡng nghiệp vụ, tuyên truyền, phổ biến nâng cao nhận thức về an toàn thông tin mạng

2. Các đơn vị tổ chức đào tạo, bồi dưỡng nghiệp vụ về an toàn thông tin cho cán bộ công nghệ thông tin, cán bộ chuyên trách an toàn thông tin mạng các đơn vị trực thuộc; đào tạo cơ bản về an toàn thông tin cho cán bộ quản lý, người sử dụng máy tính thuộc đơn vị theo kế hoạch hàng năm đã được phê duyệt.

3. Các đơn vị phải thường xuyên tổ chức các hoạt động tuyên truyền, phổ biến nâng cao nhận thức về bảo đảm an toàn, an ninh thông tin mạng đến toàn thể bộ công chức, viên chức và người lao động tại đơn vị.

4. Văn phòng Sở xây dựng trình Sở kế hoạch tuyên truyền, phổ biến nâng cao nhận thức về an toàn, an ninh thông tin mạng tại Sở và thực hiện các nội dung theo kế hoạch đã được phê duyệt.

Điều 18. Chế độ báo cáo an toàn, an ninh thông tin mạng

1. Báo cáo định kỳ:

a) Báo cáo an toàn thông tin định kỳ hàng năm gồm các nội dung quy định tại Điều 14 Thông tư số 12/2022/TT-BTTTT;

b) Báo cáo hoạt động giám sát của chủ quản HTTT định kỳ 6 tháng theo mẫu tại Phụ lục 2 Thông tư số 31/2017/TT-BTTTT.

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 đơn vị chuyên trách về an toàn thông tin của tỉnh và của Cơ quan chức năng.

3. Trách nhiệm lập, phê duyệt báo cáo

a) Các đơn vị trách nhiệm:

- Lập báo cáo an toàn thông tin mạng theo quy định tại điểm a khoản 1 điều này, gửi Sở (qua Văn phòng) trước ngày 20 tháng 11 hàng năm;

- Lập báo cáo hoạt động giám sát của chủ quản HTTT theo quy định tại điểm b khoản 1 điều này, gửi về Sở (qua Văn phòng) trước ngày 20 tháng 6 và 20 tháng 12 hàng năm;

- Báo cáo đột xuất theo hướng dẫn Sở và của Cơ quan chức năng.

b) Văn phòng chịu trách nhiệm tập hợp, tổng hợp báo cáo của các phòng, đơn vị, trình Lãnh đạo Sở phê duyệt, gửi các cơ quan quản lý nhà nước về an toàn thông tin.

Chương III TỔ CHỨC THỰC HIỆN

Điều 19. Kinh phí thực hiện

1. Kinh phí đảm bảo an toàn thông tin mạng, an ninh mạng được đảm bảo từ nguồn chi thường xuyên hàng năm, hoặc lồng ghép, tích hợp với các chương trình,

dự án, nhiệm vụ sử dụng nguồn ngân sách nhà nước và các nguồn kinh phí hợp pháp khác.

2. Căn cứ vào kế hoạch hàng năm, các đơn vị có trách nhiệm đề xuất dự toán cho các hoạt động bảo đảm an toàn thông tin mạng, an ninh mạng gửi Phòng Kế hoạch - Tài chính tổng hợp, trình cấp có thẩm quyền phê duyệt và cấp kinh phí.

Điều 21. Trách nhiệm của Văn phòng

1. Thực hiện các trách nhiệm được giao tại Quy chế này.
2. Hướng dẫn triển khai Quy chế này và các quy định liên quan của Nhà nước về an toàn thông tin mạng và an ninh mạng.
3. Tổ chức triển khai thực hiện Quy chế tại trụ sở cơ quan Sở Nông nghiệp và Môi trường.
4. Xây dựng kế hoạch, báo cáo về an toàn thông tin mạng, an ninh mạng của Sở Nông nghiệp và Môi trường.

Điều 22. Trách nhiệm của các phòng, đơn vị

1. Thực hiện các trách nhiệm được giao tại Quy chế này.
2. Tổ chức triển khai thực hiện Quy chế này tại đơn vị.
3. Thực hiện các báo cáo theo quy định, gửi Văn phòng tổng hợp, báo cáo Lãnh đạo Sở.
4. Xây dựng, triển khai Quy chế bảo đảm an toàn thông tin tại đơn vị bảo đảm phù hợp với Quy chế này và các yêu cầu cụ thể của đơn vị.
5. Vận hành hệ thống mạng nội bộ, hệ thống an toàn, an ninh mạng, các HTTT, cơ sở dữ liệu đảm bảo đúng quy định của pháp luật.

Điều 23. Trách nhiệm của chủ quản HTTT

1. Thực hiện trách nhiệm của đơn vị chủ quản HTTT theo quy định tại Quy chế này.
2. Chỉ đạo, phân công các đơn vị vận hành các HTTT triển khai công tác bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến HTTT.
3. Chỉ đạo rà soát, xác định các HTTT quan trọng về an ninh quốc gia theo Điều 3 Nghị định số 53/2022/NĐ-CP.

Điều 24. Trách nhiệm của đơn vị vận hành HTTT

1. Thực hiện trách nhiệm của đơn vị vận hành HTTT theo quy định tại Quy chế này và các nhiệm vụ do chủ quản HTTT phân công.
2. Chỉ đạo, phân công các bộ phận kỹ thuật thuộc đơn vị (quản lý mạng; quản lý ứng dụng; quản lý dữ liệu; vận hành HTTT; triển khai và hỗ trợ kỹ thuật) triển khai công tác bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến HTTT.

Điều 25. Trách nhiệm của người sử dụng, cá nhân liên quan

1. Người đứng đầu các phòng, đơn vị thuộc đối tượng áp dụng của Quy chế này có trách nhiệm: phổ biến tới từng công chức, viên chức, người lao động của đơn vị; thường xuyên kiểm tra việc thực hiện Quy chế này tại đơn vị; chịu trách nhiệm trước pháp luật và Lãnh đạo Sở về các vi phạm, thất thoát thông tin, dữ liệu thuộc phạm vi quản lý của đơn vị do không tổ chức, chỉ đạo, kiểm tra cán bộ của đơn vị thực hiện đúng quy định.

2. Công chức, viên chức, người lao động của Sở Nông nghiệp và Môi trường, các đơn vị thuộc Sở và các đơn vị khác thuộc đối tượng áp dụng của Quy chế có trách nhiệm: tuân thủ Quy chế; thông báo các vấn đề bất thường liên quan tới an toàn thông tin mạng, an ninh mạng bộ phận phụ trách về an toàn thông tin mạng của đơn vị; chịu trách nhiệm trước pháp luật và Lãnh đạo đơn vị về các vi phạm, thất thoát dữ liệu của Sở do không tuân thủ Quy chế.

3. Các tổ chức, cá nhân phải ký cam kết bảo mật đối với các thông tin quan trọng (bao gồm nhưng không giới hạn: tài liệu thiết kế thi công, thông tin cấu hình hệ thống, điểm yếu an toàn thông tin chưa được xử lý, tài khoản quản trị...) khi được giao xây dựng, triển khai, quản lý, vận hành HTTT. Ký cam kết không để lộ lọt thông tin của hệ thống được giao xây dựng, triển khai, quản lý, vận hành.

Điều 26. Khen thưởng, kỷ luật

1. Kết quả thực hiện Quy chế này là một trong những tiêu chí đánh giá kết quả thực hiện hàng năm của cá nhân, đơn vị đồng thời là tiêu chí bắt buộc để xem xét khen thưởng và danh hiệu thi đua đối với các tổ chức, cá nhân.

2. Đơn vị, cá nhân vi phạm Quy chế này và các quy định khác của pháp luật về bảo đảm an toàn, an ninh thông tin mạng, tùy theo tính chất, mức độ vi phạm sẽ bị xử lý kỷ luật hoặc các hình thức xử lý khác theo quy định của pháp luật; nếu vi phạm gây thiệt hại đến tài sản, thiết bị, thông tin, dữ liệu thì chịu trách nhiệm bồi thường theo pháp luật hiện hành.

Điều 27. Rà soát, cập nhật, bổ sung Quy chế

1. Định kỳ hàng năm hoặc khi có thay đổi chính sách an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung Quy chế bảo đảm an toàn thông tin.

2. Có hồ sơ lưu lại thông tin phản hồi của đối tượng áp dụng chính sách trong quá trình triển khai, áp dụng chính sách an toàn thông tin.

3. Trong quá trình thực hiện Quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời về Sở (qua Văn phòng Sở) để tổng hợp báo cáo Lãnh đạo Sở xem xét, điều chỉnh, bổ sung)./.
