BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG **CỤC QUẢN LÝ ĐÊ ĐIỀU VÀ PHÒNG, CHỐNG THIÊN TAI**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 450 /QĐ-ĐĐ	*Hà Nội, ngày 09 tháng 9 năm 2025*

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Quản lý đê điều và Phòng, chống thiên tai

CỤC TRƯỞNG
CỤC QUẢN LÝ ĐÊ ĐIỀU VÀ PHÒNG, CHỐNG THIÊN TAI

Căn cứ Quyết định số 198/QĐ-BNNMT ngày 01/03/2025 của Bộ trưởng Bộ Nông nghiệp và Môi trường quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Cục Quản lý đê điều và Phòng, chống thiên tai;

Căn cứ Luật An toàn thông tin mạng; Luật An ninh mạng; Luật Bảo vệ bí mật 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; số 53/2022/NĐ-CP ngày 15/8/2022 quy định chi tiết một số điều của Luật An ninh mạng; số 13/2023/NĐ-CP ngày 17/4/2023 về bảo vệ dữ liệu cá nhân và số 26/2020/NĐ-CP ngày 28/02/2020 quy định chi tiết một số điều của Luật Bảo vệ bí mật Nhà nước;

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

Căn cứ các Thông tư của Bộ Thông tin và Truyền thông số 12/2022/TT-BTTTT ngày 12/8/2022 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; số 20/2017/TT-BTTTT ngày 12/9/2017 quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc và số 31/2017/TT-BTTTT ngày 15/11/2017 quy định hoạt động giám sát an toàn hệ thống thông tin;

Căn cứ Quyết định số 1921/QĐ-BNNMT ngày 05/6/2025 của Bộ trưởng Bộ Nông nghiệp và Môi trường ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Bộ Nông nghiệp và Môi trường;

Theo đề nghị của Trưởng phòng Cơ sở dữ liệu phòng, chống thiên tai.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Quản lý đê điều và Phòng, chống thiên tai.

Điều 2. Quyết định này có hiệu lực từ ngày ký và thay thế cho Quyết định số 483/QĐ-ĐĐ-VP ngày 29/11/2023 của Cục trưởng Cục Quản lý đê điều và Phòng, chống thiên tai ban hành Quy chế an toàn thông tin mạng và an ninh mạng của Cục Quản lý đê điều và Phòng, chống thiên tai.

Điều 3. Chánh Văn phòng Cục; Trưởng phòng Cơ sở dữ liệu phòng, chống thiên tai; lãnh đạo các đơn vị, công chức, viên chức, người lao động thuộc Cục Quản lý đê điều và Phòng, chống thiên tai và tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Các Phó Cục trưởng (để chỉ đạo);
- Các đơn vị trực thuộc Cục (để thực hiện);
- Lưu: VT, CSDL.

CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC QUẢN LÝ ĐÊ ĐIỀU VÀ PHÒNG, CHỐNG THIÊN TAI
BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG

Phạm Đức Luận

BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG
CỤC QUẢN LÝ ĐÊ ĐIỀU
VÀ PHÒNG, CHỐNG THIÊN TAI

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

QUY CHẾ
BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG, AN NINH MẠNG CỦA CỤC QUẢN LÝ ĐÊ ĐIỀU VÀ PHÒNG, CHỐNG THIÊN TAI

(Kèm theo Quyết định số /QĐ-ĐĐ ngày tháng năm 2025 của Cục trưởng Cục Quản lý đê điều và Phòng, chống thiên tai)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh: Quy chế này quy định về công tác bảo đảm an toàn thông tin mạng (ATTT) và an ninh mạng (ANM) trong các hoạt động ứng dụng công nghệ thông tin (CNTT), xây dựng chính phủ điện tử, chính phủ số và chuyển đổi số của Cục Quản lý đê điều và Phòng, chống thiên tai (sau đây gọi tắt là Cục).

2. Đối tượng áp dụng

a) Các đơn vị trực thuộc Cục Quản lý đê điều và Phòng, chống thiên tai (sau đây gọi là đơn vị trực thuộc Cục) và công chức, viên chức, người lao động thuộc các đơn vị trực thuộc Cục.

b) Các cơ quan, tổ chức, cá nhân sử dụng hoặc kết nối, truy cập vào hệ thống mạng, hệ thống thông tin, cơ sở dữ liệu (CSDL) của Cục;

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ CNTT, chính phủ điện tử, chính phủ số và an toàn thông tin cho Cục và các đơn vị trực thuộc Cục.

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, 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. *An ninh mạng* là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

3. *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.

4. *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.

5. *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.

6. *Trang thiết bị CNTT* là một nhóm hay một dòng sản phẩm cố định có khả năng xử lý dữ liệu và truyền tải thông tin dữ liệu qua lại giữa những người sử dụng.

7. *Thiết bị xử lý thông tin* là thiết bị dùng để tạo lập, xử lý, lưu trữ, truyền đưa thông tin dưới dạng điện tử (máy tính, máy in, điện thoại thông minh, thiết bị mạng, thiết bị an ninh mạng, camera giám sát và các thiết bị tương đương khác).

8. *Người dùng* là công chức, viên chức, người lao động thuộc Cục; các cá nhân khác sử dụng máy tính để xử lý công việc, truy cập hệ thống thông tin, CSDL.

9. *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.

10. *Trang thông tin điện tử (website)* là trang thông tin hoặc một tập hợp trang thông tin, ứng dụng (application) trên Internet được trình bày dưới dạng ký hiệu, số, chữ viết, hình ảnh, âm thanh và các dạng thông tin khác phục vụ cho việc cung cấp, sử dụng nội dung, dịch vụ khác nhau trên Internet.

11. *Trung tâm dữ liệu/phòng máy chủ* là một tòa nhà, không gian dành riêng trong tòa nhà hoặc một nhóm các tòa nhà được sử dụng để đặt tập trung hệ thống máy chủ, thiết bị lưu trữ, thiết bị định tuyến, thiết bị chuyển mạch, thiết bị bảo đảm an toàn thông tin mạng, an ninh mạng, thiết bị ngoại vi, đường truyền kết nối internet, nguồn điện dự phòng, hệ thống làm lạnh, thiết bị phòng cháy, chữa cháy, chống sét, thiết bị hỗ trợ và các trang thiết bị khác.

12. *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.

13. *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.

14. *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.

15. *Tài sản số* của cơ quan quản lý nhà nước gồm dữ liệu số (quốc gia, chuyên ngành, mở), hệ thống thông tin và phần mềm, hạ tầng số (trung tâm dữ liệu, mạng), dịch vụ và nền tảng số, cùng với các tài sản trí tuệ số. Đây là tài sản công, thuộc sở hữu Nhà nước, được quản lý, khai thác và bảo vệ theo quy định pháp luật về công nghệ thông tin, an toàn thông tin và tài sản công.

16. *Dùng chung* được hiểu là tài sản số của cơ quan nhà nước được quản lý tập trung, công khai mức độ khai thác, không sở hữu riêng biệt, chia sẻ có kiểm soát theo

thẩm quyền; và tuân thủ các quy định của pháp luật trong lĩnh vực công nghệ thông tin, an toàn thông tin về phân quyền, bảo mật, an toàn thông tin.

17. *Chủ quản hệ thống thông tin* là cơ quan, tổ chức được giao trách nhiệm sở hữu, quản lý, tổ chức xây dựng, duy trì, phát triển và bảo đảm an toàn cho hệ thống thông tin đó.

18. 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.

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

1. Tuân thủ quy định của pháp luật về an toàn thông tin mạng; bảo vệ bí mật nhà nước, dữ liệu cá nhân; giao dịch điện tử và các quy định khác có liên quan.

2. Phân cấp, ủy quyền trách nhiệm bảo đảm an toàn thông tin mạng phù hợp với tổ chức bộ máy và phương thức làm việc của Cục.

3. An toàn thông tin mạng và an ninh mạng phải gắn liền và hỗ trợ các hoạt động giao dịch điện tử, ứng dụng CNTT, xây dựng chính phủ điện tử, chính phủ số và công tác chuyển đổi số của Cục; hỗ trợ việc sử dụng trang thiết bị CNTT, thiết bị xử lý thông tin để xử lý công việc của công chức, viên chức, người lao động

4. Các hệ thống thông tin dùng chung của Cục phải được trình cấp có thẩm quyền 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.

5. Ứng cứu sự cố an toàn thông tin mạng phải phù hợp với trách nhiệm, quyền hạn của các bên liên quan; đảm bảo các bước phát hiện, phản ứng, khắc phục và phục hồi được thực hiện nhanh chóng và hiệu quả; kết thúc xử lý cần có đánh giá và cải thiện quy trình.

6. Mỗi công chức, viên chức, người lao động tại các đơn vị thuộc Cục nêu cao tinh thần chủ động, tự giác trong việc áp dụng các biện pháp an toàn thông tin 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 đấu 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 cơ quan, đơn vị để đào tiền ảo, đánh bạc, cá độ.

5. Phát tán thư rác, phần mềm độc hại, thiết lập hệ thống thông tin 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 hệ thống thông tin 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 hệ thống thông tin hoặc tới khả năng truy cập hệ thống thông tin 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 VỀ BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN MẠNG

Điều 5. Hệ thống tài nguyên cần đảm bảo an toàn thông tin của Cục

1. Hệ thống mạng (bao gồm):

- Hệ thống đường truyền dữ liệu, đường truyền kết nối Internet;

- Hệ thống mạng có dây (LAN)/WAN, mạng không dây (Wifi);

- Trang thiết bị CNTT được kết nối mạng trong cơ quan Cục.

2. Hệ thống tài nguyên mạng và ứng dụng CNTT:

- Hệ thống thư điện tử, văn phòng điện tử dùng chung của Bộ;

- Hệ thống thông tin và CSDL do Cục, các đơn vị trực thuộc xây dựng, quản lý, vận hành;

- Trang thông tin điện tử (Website) và các trang thông tin trên mạng xã hội của Cục.

- Các phần mềm ứng dụng khác phục vụ công tác quản lý, điều hành hoạt động quản lý nhà nước thuộc phạm vi quản lý của Cục.

3. Hệ thống máy chủ, phòng máy chủ:

- Hệ thống máy chủ đặt tại số 10 Tôn Thất Thuyết, Cầu Giấy, Hà Nội;

- Hệ thống máy chủ đặt tại số 54/102, Trường Chinh, Kim Liên, Hà Nội;

- Hệ thống các máy chủ, máy chủ ảo do Cục, các đơn vị trực thuộc thuê từ các nhà cung cấp dịch vụ CNTT để cài đặt phần mềm ứng dụng, CSDL phục vụ quản lý, điều hành của Cục.

Điều 6. Bảo đảm an toàn thông tin mạng đối với hệ thống thông tin, trang thiết bị CNTT, thiết bị xử lý thông tin

1. Đơn vị chủ quản hệ thống thông tin thực hiện các nhiệm vụ:

a) Tổ chức xác định cấp độ hệ thống thông tin và xây dựng phương án bảo đảm an toàn hệ thống thông tin theo cấp độ phục vụ mục đích đánh giá an toàn thông tin và bảo đảm an toàn thông tin cho các hệ thống thông tin. Nguyên tắc bảo đảm an toàn

thông tin theo cấp độ và nguyên tắc xác định cấp độ căn cứ trên các nguyên tắc quy định tại Điều 4, Điều 5 Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ;

b) Xây dựng, trình cấp có thẩm quyền xác định cấp độ an toàn cho hệ thống thông tin theo quy định và triển khai phương án bảo đảm an toàn hệ thống thông tin theo cấp độ theo quy định.

2. Bảo đảm an toàn, an ninh thông tin khi sử dụng máy tính:

a) Các đơn vị trực thuộc và công chức, viên chức, người lao động trong các đơn vị (sau đây gọi chung là người sử dụng) chỉ cài đặt phần mềm có hỗ trợ cập nhật các bản vá lỗi, tính năng mới, bản vá lỗ hổng bảo mật; không tự ý cài đặt hoặc gỡ bỏ các phần mềm đã được cài đặt trên máy tính; 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; phòng, chống virus 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 người có thẩm quyền để được xử lý, hướng dẫn triển khai xử lý kịp thời;

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

3. Bảo đảm an toàn, an ninh thông tin đối với máy chủ:

a) Chỉ cài đặt và sử dụng các phần mềm có 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 cập nhật bản vá bảo mật khi không thực sự cần thiết;

b) 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;

c) Triển khai các biện pháp sao lưu dự phòng để nâng cao khả năng phục hồi hoạt động khi xảy ra sự cố. Đối với các hệ thống thông tin quan trọng (VNDMS, Webgis đê điều, webgis sạt lở bờ sông bờ biển,…) cần thực hiện quy tắc sao lưu dự phòng 3-2-1: có 03 bản sao lưu dự phòng; lưu trữ ít nhất trên 02 loại phương tiện khác nhau; 01 bản được lưu trữ offline. Định kỳ kiểm tra tính toàn vẹn và khả năng khôi phục thành công hệ thống từ các bản sao lưu.

d) Giám sát thường xuyên, liên tục các máy chủ, đặc biệt là các truy cập đến máy chủ cung cấp dịch vụ nền tảng như vCenter, ESXI, Domain Controller… để phát hiện và cảnh báo sớm nguy cơ mất an toàn thông tin.

e) Định kỳ tìm kiếm, đánh giá, điều tra các dấu hiệu tấn công mạng, rà quét mã độc trên toàn bộ hệ thống. Thông báo và phối hợp với các đầu mối ứng cứu sự cố an toàn thông tin của Cục để xử lý nếu phát hiện thấy bất thường trong hệ thống.

f) Các hệ thống thông tin, phần mềm ứng dụng, dịch vụ cài đặt trên máy chủ

- Không được cài các phần mềm điều khiển máy tính từ xa của bên thứ 3 như TeamViewer, AnyDesk, UltraViewer…

- Hệ thống thông tin, phần mềm ứng dụng phải đáp ứng các yêu cầu sau: cấu hình 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.

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

- Ghi và lưu giữ bản ghi nhật ký hệ thống của hệ thống thông tin, phần mềm ứng dụng trong khoảng thời gian tối thiểu 03 tháng với những thông tin cơ bản: thời gian, địa chỉ kết nối, tài khoản (nếu có), nội dung truy cập dữ liệu, dịch vụ; các lỗi phát sinh trong quá trình hoạt động; thông tin đăng nhập khi quản trị, thông tin thay đổi cấu hình máy chủ.

- Cần được 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. Định kỳ thực hiện quy trình kiểm soát cài đặt, cập nhật, vá các điểm yếu bảo mật của hệ thống thông tin, phần mềm ứng dụng, dịch vụ trên các máy chủ.

4. Bảo đảm an toàn thông tin đối với hệ thống mạng máy tính:

a) Hệ thống mạng nội bộ (LAN) 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 mạng, thiết bị bảo mật;

b) Triển khai áp dụng các biện pháp kỹ thuật cần thiết bảo đảm an toàn thông tin trong hoạt động kết nối 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 (VPN) thông dụng và có phần cứng mã hóa tích hợp để tăng tốc độ mã hóa dữ liệu và có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ (DDoS); lọc bỏ, không cho phép truy nhập các trang/cổng thông tin có nghi ngờ chứa mã độc hoặc các nội dung không phù hợp;

c) Các đường truyền dữ liệu, đường truyền Internet và các hệ thống dây dẫn các mạng LAN, WAN chạy trong các tòa nhà và phòng làm việc phải được lắp đặt trong ống, có nắp che đậy kín, hạn chế khả năng tiếp cận trái phép. Ngắt kết nối cổng Ethernet không sử dụng, đặc biệt là ở khu vực làm việc chung;

5. Bảo đảm an toàn thông tin đối với trung tâm dữ liệu/phòng máy chủ:

a) Các thiết bị kết nối mạng, thiết bị bảo mật quan trọng như tường lửa (firewall), thiết bị định tuyến (router), thiết bị chuyển mạch (switch), hệ thống máy

chủ, hệ thống lưu trữ SAN, NAS,... phải được đặt trong trung tâm dữ liệu/phòng máy chủ và phải được thiết lập cơ chế bảo vệ, theo dõi phát hiện xâm nhập và biện pháp kiểm soát truy nhập, kết nối vật lý phù hợp với từng khu vực: máy chủ và hệ thống lưu trữ; tủ mạng và đầu nối; thiết bị nguồn điện và dự phòng điện khẩn cấp; vận hành, kiểm soát, quản trị hệ thống.

b) Trung tâm dữ liệu/phòng máy chủ là khu vực hạn chế tiếp cận chỉ những cá nhân có quyền, nhiệm vụ theo quy định của Cục trưởng, của thủ trưởng đơn vị quản lý mới được phép vào trung tâm dữ liệu/phòng máy chủ;

c) Trung tâm dữ liệu/phòng máy chủ phải có hệ thống làm mát điều hòa không khí, độ ẩm để đảm bảo môi trường vận hành; hệ thống cảnh báo cháy, thiết bị phòng cháy, chữa cháy khẩn cấp; hệ thống cảnh báo hệ thống nguồn điện; hệ thống chống sét lan truyền theo quy định.

d) Phải có hệ thống giám sát và đảm bảo an toàn phù hợp với yêu cầu của từng cấp độ an toàn theo quy định tại Phụ lục A - Yêu cầu cơ bản về an toàn vật lý cho hệ thống thông tin theo cấp độ tại TCVN 11930:2017.

e) Thiết lập cơ chế dự phòng đối với các thiết bị hạ tầng kỹ thuật quan trọng; có kế hoạch kiểm tra, bảo dưỡng định kỳ để duy trì thông số kỹ thuật các thiết bị này hoặc có phương án sửa chữa, thay thế đáp ứng yêu cầu về độ sẵn sàng trong suốt thời gian vận hành.

f) Các đơn vị được giao quản trị, vận hành Trung tâm dữ liệu/phòng máy chủ có trách nhiệm xây dựng nội quy hoặc hướng dẫn làm việc tại khu vực này; cử cán bộ thường xuyên giám sát thiết bị, hạ tầng của Trung tâm dữ liệu/phòng máy chủ.

Điều 7. Quản lý an toàn thông tin khi xây dựng, tiếp nhận, phát triển, vận hành và bảo trì hệ thống thông tin

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

2. Khi xây dựng, tiếp nhận, phát triển, nâng cấp, bảo trì hệ thống thông tin, 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.

3. Tách biệt với các môi trường phát triển, kiểm tra và thử nghiệm. Các vùng mạng này không được kết nối ra ngoài internet. Nếu quá trình thử nghiệm bắt buộc phải có kết nối ra ngoài internet thì phải đăng ký đơn vị chuyên trách về an toàn thông tin của Cục để triển khai các thủ tục thiết lập chỉ cho phép kết nối đến đúng địa chỉ IP, đường dẫn URL (Uniform Resource Locator), các cổng kết nối cần thiết trong khoảng thời gian cho phép.

4. Trong quá trình vận hành hệ thống thông tin, đơn vị chủ quản hệ thống thông tin cần thực hiện đánh giá, phân loại hệ thống thông tin theo cấp độ; triển khai phương

án bảo đảm an toàn hệ thống thông tin đáp ứng yêu cầu cơ bản trong tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm an toàn hệ thống thông tin theo cấp độ; thường xuyên kiểm tra, giám sát an toàn hệ thống thông tin; tuân thủ quy trình vận hành, quy trình xử lý sự cố đã xây dựng; ghi lại và lưu trữ đầy đủ thông tin nhật ký hệ thống để phục vụ quản lý, kiểm soát thông tin.

5. Các đơn vị thuộc Cục liên quan đến việc phát triển phần mềm ứng dụng có trách nhiệm yêu cầu các đối tác (nếu có) thực hiện các công tác bảo đảm an toàn thông tin, tránh lộ, lọt mã nguồn và dữ liệu, tài liệu thiết kế, quản trị hệ thống mà đối tác đang xử lý ra bên ngoài.

Điều 8. Quản lý an toàn thông tin đối với tài khoản truy cập

1. Tài khoản truy cập (gọi tắt là tài khoản) là tập hợp gồm tên đăng nhập và mật khẩu hoặc/và hình thức xác thực khác, được gắn với quyền truy cập thực hiện một số tác vụ trên hệ thống thông tin hoặc trên thiết bị xử lý thông tin do Cục quản lý; bao gồm các loại sau:

a) Tài khoản truy cập hệ thống gắn với một nhiệm vụ cụ thể, được gắn với quyền truy cập thực hiện các tác vụ cần thiết cho nhiệm vụ đó (ví dụ: tài khoản văn thư, tài khoản biên tập,...). Người sử dụng; các cơ quan, đơn vị, cá nhân khác truy cập vào các hệ thống thông tin, CSDL của Cục được cấp và sử dụng tài khoản truy nhập với định danh duy nhất gắn với đơn vị, cá nhân đó.

b) Tài khoản quản trị gắn với quyền cài đặt, cấu hình các thông số và cấp quyền truy cập trên hệ thống thông tin, gồm: quản trị nội dung, quản trị ứng dụng, quản trị cơ sở dữ liệu, quản trị hệ điều hành, quản trị thiết bị. Đối tượng được cấp và sử dụng tài khoản truy nhập với định danh duy nhất gắn với đối tượng đó.

2. Tài khoản quản trị được giao cho cá nhân, đơn vị thực hiện nhiệm vụ quản trị ứng dụng, quản trị cơ sở dữ liệu, quản trị hệ điều hành, quản trị thiết bị. Phòng Cơ sở dữ liệu phòng, chống thiên tai (Phòng Cơ sở dữ liệu PCTT) và Trung tâm Chính sách và Kỹ thuật phòng chống thiên tai (Trung tâm CS&KT) giữ ít nhất 01 tài khoản quản trị hệ điều hành của tất cả các máy chủ hoạt động trong mạng nội bộ Cục.

3. Quy định về mật khẩu của tài khoản truy cập:

a) Mật khẩu tài khoản truy cập hệ thống cho người dùng, phải đáp ứng các yêu cầu: có tối thiểu 8 ký tự, 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 khác trên bàn phím máy tính (` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ I : ; " ' < > , . ? /) và dấu cách; không chứa tên tài khoản; mật khẩu phải được thay đổi tối thiểu 12 tháng một lần.

b) Mật khẩu tài khoản quản trị phải đáp ứng các yêu cầu: có tối thiểu 15 ký tự, gồm tối thiểu 3 trong 5 loại ký tự sau: chữ cái viết hoa (A - Z); chữ cái viết thường (a - z); chữ số (0 - 9); các ký tự khác trên bàn phím máy tính (' ~ ! @ # $ % ^ & * () _ - + = { } [ ] \ I : ; “ ‘ <> , . ? /) và dấu cách; không chứa tên tài khoản; mật khẩu phải được thay đổi tối thiểu 06 tháng một lần.

4. Cá nhân được cấp hoặc giao tài khoản chịu trách nhiệm về các hành vi của tài khoản được ghi nhận trên thiết bị xử lý thông tin, hệ thống thông tin, hệ thống

giám sát an toàn thông tin mạng. Trường hợp thay đổi vị trí công tác, chuyển công tác, nghỉ hưu, thôi việc, trong thời hạn 05 ngày làm việc (kể từ thời điểm có quyết định chính thức) đơn vị quản lý cá nhân đó phải thông báo về Văn phòng Cục để điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng tài khoản được cấp; trường hợp hệ thống thông tin, CSDL 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, nghỉ hưu, thôi việc thì không phải thông báo về Văn phòng Cục.

5. Đơn vị vận hành hệ thống thông tin thường xuyên rà soát các tài khoản truy cập hệ thống đang hoạt động, phát hiện và thu hồi các tài khoản không sử dụng hoặc không hợp lệ, điều chỉnh thông tin tài khoản chưa phản ánh chính xác thông tin thực tế tại thời điểm rà soát.

Điều 9. Quy định về bảo đảm 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: 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 nhập, 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.

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.

a) Phần mềm, ứng dụng phải được kiểm tra, phát hiện và khắc phục các điểm yếu về an toàn, an ninh thông tin mạng trước khi đưa vào sử dụng và trong quá trình sử dụng;

b) 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 của Cục.

Điều 10. Quản lý an toàn, an ninh thông tin đối với dữ liệu

1. Các đơn vị trực thuộc Cục 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 đơn vị trực thuộc Cục 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, 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 đơn vị trực thuộc Cục 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 của Chính phủ 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 11. Quản lý an toàn thông tin đối với cán bộ, công chức, viên chức và người lao động tham gia công tác bảo đảm an toàn thông tin mạng

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

a) Có phẩm chất đạo đức tốt, 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.

c) Đối với các vị trí tiếp xúc, quản lý các thông tin, dữ liệu quan trọng hoặc quản trị các hệ thống thông tin quan trọng, nhân sự phải có 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 trong quá trình công tác và sau khi thôi việc tại đơn vị.

2. Khi cán bộ, công chức, viên chức và người lao động chấm dứt hoặc thay đổi công việc, các đơn vị phải:

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

b) Thay đổi hoặc thu hồi quyền truy cập các hệ thống thông tin.

c) 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 hệ thống thông tin để bảo đảm tài khoản người dùng của, công chức, viên chức và người lao động đã nghỉ việc được thu hồi.

Điều 12. Giám sát an toàn thông tin mạng

1. Giao Phòng Cơ sở dữ liệu PCTT chủ trì, phối hợp với các đơn vị thực hiện giám sát an toàn thông tin mạng cho toàn bộ hạ tầng công nghệ thông tin dùng chung của Bộ, mạng nội bộ và mạng không dây do Cục quản lý.

2. Các hệ thống thông tin bắt buộc phải có chức năng ghi và lưu trữ nhật ký về hoạt động của hệ thống và người sử dụng hệ thống thông tin. 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 ngày 15/11/2017 của Bộ Thông tin và Truyền thông.

4. Thông báo cho các đầu mối ứng cứu sự cố của Cục và đơn vị vận hành hệ thống thông tin khi phát hiện hệ thống thông tin đang bị tấn công mạng; ngắt kết nối mạng hoặc tắt máy chủ, máy trạm đang bị lây nhiễm mã độc để hạn chế thiệt hại và mất mát thông tin, dữ liệu.

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

1. Phòng Cơ sở dữ liệu PCTT có thẩm quyền yêu cầu kiểm tra, đánh giá an toàn thông tin mạng đối với các hệ thống thông tin.

2. Nội dung, hình thức kiểm tra, đánh giá theo quy định tại Điều 11 và Điều 12 Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông.

3. Phòng Cơ sở dữ liệu PCTT chủ trì, phối hợp với các đơn vị thực hiện việc đánh giá hiệu quả các biện pháp bảo đảm an toàn thông tin theo thẩm quyền. Nội dung đánh giá là cơ sở để điều chỉnh phương án bảo đảm an toàn thông tin cho phù hợp.

Điều 14. Ứng cứu sự cố an toàn thông tin mạng

1. Phòng Cơ sở dữ liệu PCTT chủ trì, phối hợp với các đơn vị, có trách nhiệm theo dõi, nắm bắt thông tin từ Cục Chuyển đổi số về các sự kiện mất an toàn thông tin mạng có thể tác động tới hệ thống thông tin của Cục; chủ động kiểm tra, rà soát theo các văn bản cảnh báo, hướng dẫn của các cơ quan chức năng và các tổ chức về an toàn thông tin; Thiết lập kênh trao đổi thông tin với các đối tác cung cấp thiết bị, phần mềm, giải pháp an toàn thông tin của đơn vị để nắm bắt kịp thời vấn đề, sự cố có khả năng tác động tới hệ thống thông tin.

2. Các đơn vị vận hành rà soát, đánh giá các rủi ro và sự cố an toàn thông tin (phân loại theo sự cố thông thường và sự cố nghiêm trọng) có thể xảy ra để xây dựng, trình Cục phê duyệt phương án và quy trình ứng cứu sự cố cho hệ thống thông tin trong phạm vi quản lý.

3. Khi phát hiện sự cố an toàn thông tin mạng thuộc loại hình tấn công mạng, đơn vị vận hành hệ thống thông tin phải thông báo tới Phòng Cơ sở dữ liệu PCTT để cùng phối hợp điều tra và khắc phục sự cố.

4. Quy trình ứng cứu sự cố an toàn thông tin mạng được thực hiện theo Khoản 3 Điều 17 Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng tại Quyết định số 1921/QĐ-BNNMT ngày 5 tháng 6 năm 2025 của Bộ Nông nghiệp và Môi trường.

5. Các đơn vị cử cán bộ tham gia đội Ứng phó sự cố của Cục và thực hiện đầy đủ các cuộc diễn tập về ứng cứu sự cố an toàn thông tin mạng khi có tập huấn của Bộ.

6. Các đơn vị vận hành hệ thống thông tin cử 01 lãnh đạo đơn vị và ít nhất 01 chuyên viên làm đầu mối ứng cứu sự cố để tiếp nhận cảnh báo, cung cấp, trao đổi, chia sẻ thông tin với Phòng Cơ sở dữ liệu PCTT trong các hoạt động giám sát an toàn thông tin mạng, ứng phó sự cố tại đơn vị và tại Cục.

Điều 15. Phổ biến, tuyên truyền, đào tạo, bồi dưỡng về an toàn thông tin mạng

1. Phòng Cơ sở dữ liệu PCTT chủ trì, phối hợp với Văn phòng Cục và các đơn vị liên quan lập kế hoạch và triển khai công tác tuyên truyền, phổ biến chủ trương, chính sách, pháp luật, biện pháp an toàn thông tin mạng, thông qua các hình thức: văn bản, gửi thư điện tử và các hình thức khác phù hợp với quy định của pháp luật. Các đơn vị thuộc Cục có trách nhiệm thực hiện quán triệt, tuyên truyền, phổ biến, nâng cao nhận thức, trách nhiệm về an toàn thông tin mạng cho cán bộ, công chức, viên chức, người lao động thuộc đơn vị.

2. Phòng Cơ sở dữ liệu PCTT chủ trì, phối hợp với Văn phòng Cục và các đơn vị liên quan tổ chức đào tạo, bồi dưỡng theo các chương trình đào tạo ngắn hạn nâng cao kiến thức, kỹ năng về an toàn thông tin mạng cho công chức, viên chức, người lao động.

Điều 16. Chế độ báo cáo

1. Báo cáo định kỳ:

a) Báo cáo an toàn thông tin định kỳ hàng năm trước ngày 10 tháng 11 gồm các nội dung quy định tại Điều 13, Điều 14 Thông tư 12/2022/TT-BTTTT.

b) Báo cáo hoạt động giám sát của chủ quản hệ thống thông tin định kỳ 6 tháng trước ngày 10 tháng 6 và 10 tháng 12 hàng năm theo mẫu tại Phụ lục 2 Thông tư 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 các cơ quan quản lý nhà nước về an toàn thông tin.

3. Trách nhiệm lập, phê duyệt báo cáo

a) Các đơn vị trực thuộc Cục đang quản lý hệ thống thông tin có trách nhiệm lập báo cáo định kỳ, báo cáo đột xuất theo yêu cầu theo nội dung quy định tại khoản 1 Điều này gửi Phòng Cơ sở dữ liệu PCTT.

b) Phòng Cơ sở dữ liệu PCTT chịu trách nhiệm tập hợp, tổng hợp báo cáo của các đơn vị quy định tại điểm a, khoản 3 Điều này, trình Lãnh đạo Cục duyệt, gửi Cục Chuyển đổi số trước ngày 20/6 và 20/12 hàng năm để tổng hợp, báo cáo Bộ.

Chương III
TỔ CHỨC THỰC HIỆN

Điều 17. Kinh phí thực hiện

Kinh phí bảo đảm an toàn thông tin mạng, an ninh mạng được lấy từ nguồn ngân sách nhà nước dự toán hàng năm của Cục Quản lý đê điều và Phòng, chống thiên tai theo quy định tại Điều 20 Quyết định số 1921/QĐ-BNNMT ngày 5 tháng 6 năm 2025 của Bộ trưởng Bộ Nông nghiệp và Môi trường về việc ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Bộ Nông nghiệp và Môi trường.

Căn cứ vào kế hoạch hàng năm, các đơn vị liên quan 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 để tổng hợp, trình cấp có thẩm quyền phê duyệt.

Điều 18. Trách nhiệm của Lãnh đạo Cục

1. Cục trưởng chịu trách nhiệm của người đứng đầu về công tác bảo đảm an toàn thông tin trước Bộ trưởng và pháp luật.

2. Phó Cục trưởng phụ trách an toàn thông tin chịu trách nhiệm:

a) Chỉ đạo, đôn đốc các đơn vị trực thuộc Cục tuyên truyền, phổ biến, thực hiện và tuân thủ các quy định tại Quy chế này.

b) Chỉ đạo, phân công các đơn vị vận hành các hệ thống thông tin triển khai công tác bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

c) Chủ trì công tác thẩm định, trình phê duyệt, phê duyệt hồ sơ đề xuất cấp độ và phương án bảo đảm an toàn thông tin theo quy định tại Nghị định số 85/2016/NĐ-CP.

d) Chỉ đạo công tác đào tạo, bồi dưỡng, tăng cường năng lực cho bộ phận chuyên trách về an toàn thông tin và các nhân làm công tác an toàn thông tin.

Điều 19. Trách nhiệm của các đơn vị thuộc Cục

1. Tổ chức triển khai thực hiện trách nhiệm được giao trong Quy chế này tại đơn vị.

2. Xây dựng, triển khai Quy chế bảo đảm an toàn, an ninh thông tin cho các hệ thống thông tin trong phạm vi quản lý, bảo đảm phù hợp với Quy chế này và các yêu cầu cụ thể của đơn vị.

3. Thực hiện việc quản lý trang thiết bị công nghệ thông tin và công chức, viên chức, người lao động theo Quy chế này.

4. Xác định các yêu cầu và trách nhiệm cụ thể của bộ phận, cán bộ, nhân viên trong việc bảo đảm an toàn, an ninh thông tin cho từng vị trí phân công.

5. Thực hiện đúng quy trình cấp mới, quản lý và thu hồi tài khoản, phân quyền truy cập các hệ thống thông tin và tất cả các tài sản liên quan đến hệ thống thông tin đối với các cá nhân do đơn vị quản lý theo quy chế này. Thường xuyên rà soát, kiểm tra quyền truy cập vào các hệ thống thông tin đối với tất cả cán bộ, công chức, viên chức và người lao động bảo đảm quyền truy cập phù hợp với nhiệm vụ được giao.

6. Thường xuyên tổ chức các hoạt động tuyên truyền, phổ biến nâng cao nhận thức về bảo đảm an toàn, an ninh thông tin; nhận diện, cảnh giác, phòng ngừa và ngăn chặn các hoạt động vi phạm pháp luật trên không gian mạng đến toàn thể công chức, viên chức và người lao động tại đơn vị.

Điều 20. Trách nhiệm của Phòng Cơ sở dữ liệu phòng, chống thiên tai

1. Thực hiện trách nhiệm của đơn vị đầu mối về an toàn thông tin theo quy định tại Điều 21 Nghị định 85/2016/NĐ-CP, Quy chế này và các nhiệm vụ do Lãnh đạo Cục phân công.

2. Theo dõi, đôn đốc, giám sát, kiểm tra và báo cáo Cục việc thực hiện Quy chế này tại các đơn vị thuộc Cục.

3. Tổ chức các hoạt động tuyên truyền, phổ biến nâng cao nhận thức về an toàn thông tin, an ninh mạng; nhận diện, cảnh giác, phòng ngừa và ngăn chặn các hoạt động vi phạm pháp luật trên không gian mạng tại Cục, lồng ghép trong các chương trình hội nghị, tập huấn, hội thảo về ứng dụng công nghệ thông tin và chuyển đổi số của lĩnh vực đê điều, phòng, chống thiên tai.

4. Đôn đốc, giám sát thực hiện bảo đảm an toàn thông tin mạng cho các hệ thống thông tin, cơ sở dữ liệu dùng chung, trọng yếu của Cục.

5. Là đầu mối tiếp nhận và phối hợp khắc phục sự cố an toàn thông tin trong Cục, theo dõi tổng hợp danh sách sự cố và tình trạng khắc phục, tham mưu cục trong công tác báo cáo định kỳ hàng năm.

6. Tổ chức rà soát định kỳ hàng năm để kiểm tra tính phù hợp của Quy chế này với các quy định của pháp luật về an toàn thông tin mạng, an ninh mạng và các quy định, tiêu chuẩn liên quan; báo cáo Lãnh đạo Cục về việc sửa đổi, bổ sung Quy chế trong trường hợp cần thiết.

Điều 21. Trách nhiệm của đơn vị vận hành hệ thống thông tin

1. Thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo quy định tại Điều 22 Nghị định 85/2016/NĐ-CP, Quy chế này và các nhiệm vụ do Cục phân công.

2. Chỉ đạo, phân công các bộ phận kỹ thuật thuộc đơn vị (quản lý ứng dụng; quản lý dữ liệu; vận hành hệ thống thông tin; 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 hệ thống thông tin.

Điều 22. Trách nhiệm của người sử dụng, cá nhân liên quan

1. Thủ trưởng đơn vị thuộc đối tượng áp dụng của Quy chế này có trách nhiệm: Tổ chức 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 Cục về các vi phạm, thất thoát thông tin, dữ liệu mật 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 Cục, các đơn vị trực thuộc Cục và các đơn vị khác thuộc đối tượng áp dụng của Quy chế có trách nhiệm: tuân thủ Quy chế; thông báo các dấu hiệu mất an toàn thông tin cho đơn vị, bộ phận đầu mối 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 quan trọng hoặc dữ liệu mật của ngành nông nghiệp và môi trường do không tuân thủ Quy chế.

Điều 23. 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 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 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 24. Trách nhiệm thi hành

1. Thủ trưởng các đơn vị trực thuộc Cục có trách nhiệm phổ biến, quán triệt đến toàn bộ công chức, viên chức, người lao động trong đơn vị thực hiện các quy định của Quy chế này.

2. Trong quá trình thực hiện, nếu có những vấn đề khó khăn, vướng mắc, các đơn vị phản ánh về Phòng Cơ sở dữ liệu PCTT để tổng hợp, trình Cục trưởng xem xét, sửa đổi, bổ sung Quy chế./.