BỘ NÔNG NGHIỆP
VÀ PHÁT TRIỂN NÔNG THÔN
CỤC QUẢN LÝ ĐÊ ĐIỀU
VÀ PHÒNG, CHỐNG THIÊN TAI

Số: 483 /QĐ-ĐĐ-VP

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

Hà Nội, ngày 29 tháng 11 năm 2023

QUYẾT ĐỊNH
V/v ban hành Quy chế An toàn thông tin mạng và An ninh mạng của 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 479/QĐ-BNN-TCCB ngày 09/02/2023 của Bộ trưởng Bộ Nông nghiệp và Phát triển nông thôn 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 Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 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; 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 3747/QĐ-BNN-KHCN ngày 05/9/2023 của Bộ Nông nghiệp và Phát triển nông thôn ban hành Quy chế An toàn thông tin mạng và An ninh mạng Bộ Nông nghiệp và Phát triển nông thôn;

Theo đề nghị của Chánh Văn phòng Cục.

QUYẾT ĐỊNH:

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

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

Điều 3. Chánh Văn phòng Cục, Thủ trưởng các đơn vị trực thuộc và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- TT Nguyễn Hoàng Hiệp (để b/c);
- Lãnh đạo Cục;
- Các đơn vị thuộc Cục;
- Trung tâm CĐS;
- Lưu: VT,VP.

CỤC TRƯỞNG

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

Phạm Đức Luận

BỘ NÔNG NGHIỆP
VÀ PHÁT TRIỂN NÔNG THÔN
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
An toàn thông tin mạng và An ninh mạng của Cục Quản lý đê điều và Phòng, chống thiên tai

(Ban hành kèm theo Quyết định số /QĐ-ĐĐ-VP ngày / /2023 của Cục Quản lý đê điều và Phòng, chống thiên tai)

Chương I
QUI ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và 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. Quy chế này áp dụng đối với:

a) Các cơ quan, đơn vị trực thuộc; công chức, viên chức, người lao động (sau đây gọi tắt là công chức, viên chức) 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) Các 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

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 hai 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 CSDL 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 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 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* tích hợp các kênh thông tin, các dịch vụ và ứng dụng theo một phương thức thống nhất, thông qua một điểm truy cập duy nhất đối với người sử dụng (từ nay gọi chung là website).

11. *Trung tâm dữ liệu/phòng máy chủ* là không gian dành riêng để lắp đặt tập trung máy chủ, 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,... và các thiết bị hỗ trợ, trang thiết bị khác.

12. *Đơn vị chủ quản hệ thống thông tin* là đơn vị được giao chủ trì xây dựng, quản lý, vận hành các hệ thống thông tin, CSDL, phần mềm ứng dụng trên Internet, trên thiết bị di động về lĩnh vực đê điều, phòng, chống thiên tai phục vụ công tác tham mưu, chỉ đạo, điều hành của Cục.

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

1. Bảo đảm an toàn, an ninh thông tin mạng và an ninh mạng là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt quá trình liên quan đến thông tin, đồng bộ từ khi thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ hệ thống thông tin (dừng hoạt động). Bảo đảm an toàn, an ninh thông tin mạng và an ninh mạng phải tuân thủ các nguyên tắc chung, được quy định tại Điều 4 Luật An ninh mạng, Điều 4 Luật An toàn thông tin mạng và Điều 4 Nghị định số 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ.

2. Việc phân cấp, ủy quyền trách nhiệm bảo đảm an toàn, an ninh mạng phải 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.

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.

6. Công chức, viên chức tại các đơn vị trực thuộc Cục nêu cao tinh thần chủ động, tự giác trong việc áp dụng các biện pháp bảo đảm an toàn, an ninh mạng và các quy định trong Quy chế này.

Điều 4. Các hành vi bị nghiêm cấm

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

2. Tự ý đấu nối thiết bị xử lý thông tin, thiết bị phát sóng như điểm truy cập mạng không dây vào mạng nội bộ của Cục, của các đơn vị thuộc Cục; trên cùng một thiết bị thực hiện đồng thời truy cập vào mạng nội bộ (LAN) và truy cập Internet bằng thiết bị kết nối Internet cá nhân (modem quay số, USB 3G/4G/5G, điện thoại di động, máy tính bảng, máy tính xách tay,…).

3. Tự ý thay đổi, gỡ bỏ biện pháp an toàn an ninh thông tin đã được cài đặt trên thiết bị CNTT phục vụ công vụ của Cục; tự ý thay thế, lắp mới, tráo đổi các linh kiện trong máy tính công vụ.

4. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin; ngăn chặn việc truy nhập đến thông tin của đơn vị, cá nhân khác trên môi trường mạng, trừ trường hợp pháp luật cho phép.

5. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của đơn vị, cá nhân khác trên môi trường mạng.

6. Các hành vi khác làm mất an toàn, an ninh, bí mật thông tin của đơn vị, 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 quản lý và CSDL chuyên ngành về đê điều, phòng, chống thiên tai do Cục, các đơn vị trực thuộc xây dựng, quản lý, vận hành;

- Trang thông tin điện tử (Website) của Cục, của Văn phòng thường trực Ban Chỉ đạo quốc gia về Phòng, chống thiên tai; các trang thông tin trên mạng xã hội (facebook, zalo, viber,…) của Cục, của Văn phòng thường trực Ban Chỉ đạo;

- 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 nhà A4, Số 2, Ngọc Hà, Ba Đình, Hà Nội;

- Hệ thống máy chủ đặt tại số 54/102, Trường Chinh, Đống Đa, 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, của Ban Chỉ đạo.

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 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 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.

4. 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. Đơn vị quản lý trung tâm dữ liệu/phòng máy chủ có trách nhiệm xây dựng nội quy hoặc hướng dẫn làm việc khu vực này;

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.

Điều 7. Quy định về quản lý tài khoản truy cập

1. 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.

2. Trường hợp người sử dụng (là cá nhân) 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.

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

4. Đơn vị chủ quản hệ thống thống tin thực hiện việc khóa quyền truy cập của tài khoản khi có chỉ đạo của lãnh đạo Cục hoặc trong trường hợp tài khoản đó thực hiện các hành vi tấn công hoặc để xảy ra, nguy cơ xảy ra vấn đề mất an toàn, an ninh thông tin mạng.

5. Quy định về sử dụng mật khẩu:

Việc đặt mật khẩu truy cập, sử dụng, quản trị hệ thống thông tin, CSDL; truy cập thiết bị lưu khóa bí mật và các tài khoản liên quan khác phục vụ công tác phải bảo đảm quy tắc:

a) Dài tối thiểu 8 ký tự, bao gồm: chữ hoa, chữ thường, số và ký tự đặc biệt;

b) Mật khẩu của người sử dụng, người quản trị hệ thống phải được đổi ngay sau khi nhận bàn giao từ người khác hoặc có thông báo về sự cố an toàn thông tin, điểm yếu liên quan đến khả năng lộ, lọt mật khẩu; mật khẩu phải được định kỳ thay đổi theo khuyến cáo của cơ quan, tổ chức thiết kế, xây dựng phần mềm, CSDL;

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

Điều 8. Quy định về bảo đảm an toàn thông tin mức 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 9. Quy định về bảo đảm an toàn thông tin mức dữ liệu

1. Các đơn vị thuộc Cục phải thực hiện biện pháp bảo vệ thông tin, dữ liệu liên quan đến hoạt động công vụ của đơn vị đặc biệt là các thông tin có nội dung quan trọng, thông tin không được công khai hoặc hạn chế công khai trên môi trường mạng.

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

Đối với hoạt động trao đổi thông tin, dữ liệu với bên ngoài, đơn vị và cá nhân thực hiện phải cam kết và có biện pháp bảo mật thông tin, dữ liệu được trao đổi. 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.

2. Đơn vị chủ quản hệ thống thông tin cần triển khai hệ thống hoặc phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản như: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, CSDL; dữ liệu, thông tin nghiệp vụ.

Điều 10. Giám sát, kiểm tra, đánh giá an toàn thông tin mạng

1. Các hệ thống thông tin, CSDL do các đơn vị xây dựng, quản lý, vận hành phải được giám sát và thường xuyên kiểm tra, đánh giá mức độ an toàn thông tin theo quy định của Bộ Thông tin và Truyền thông.

2. Các hệ thống thông tin, CSDL bắt buộc phải có chức năng ghi và lưu trữ nhật ký về hoạt động của hệ thống và người sử dụng truy cập hệ thống.

3. Đơn vị chủ quản hệ thống thông tin tự thực hiện việc giám sát, kiểm tra, đánh giá an toàn thông tin hoặc phối hợp với Văn phòng Cục để phối hợp với Trung tâm Chuyển đổi số và Thống kê nông nghiệp thực hiện giám sát và định kỳ kiểm tra, đánh giá mức độ an toàn thông tin mạng.

Điều 11. Quy định về ứng cứu sự cố an toàn thông tin mạng

a) Các đơn vị, cá nhân khi phát hiện dấu hiệu bị tấn công mạng hoặc sự cố an toàn thông tin mạng cần nhanh chóng báo cho đơn vị quản lý, vận hành hệ thống thông tin, CSDL biết để có phương án xử lý;

b) Khi xảy ra sự cố an toàn thông tin mạng thuộc loại hình tấn công mạng, đơn vị quản lý, vận hành hệ thống thông tin, CSDL thực hiện việc báo cáo sự cố theo quy

định tại điểm a, khoản 1, Điều 11 Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ và Điều 9 Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông đồng thời phối hợp với Văn phòng Cục báo cáo Trung tâm Chuyển đổi số và Thống kê nông nghiệp để tổng hợp, báo cáo Ban Chỉ đạo Chuyển đổi số của Bộ.

Điều 12. Chế độ thông tin, báo cáo

1. Trước ngày 15 tháng 11 hàng năm, các đơn vị chủ quản hệ thống thông tin báo cáo Cục trưởng (qua Văn phòng Cục) về nội dung đảm bảo an toàn thông tin theo quy định khoản 2 đến khoản 10, Điều 14 Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông.

2. Định kỳ 6 tháng hoặc đột xuất (khi có sự cố), các đơn vị chủ quản hệ thống thông tin: 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 gửi về Văn phòng Cục.

Chương III
TỔ CHỨC THỰC HIỆN

Điều 13. Trách nhiệm của các đơn vị trực thuộc Cục

1. Trách nhiệm của Văn phòng Cục:

a) Chủ trì, phối hợp với các đơn vị có liên quan tham mưu, xây dựng hồ sơ đánh giá cấp độ an toàn hệ thống thông tin trình cấp có thẩm quyền phê duyệt.

b) Chủ trì triển khai các biện pháp đảm bảo an toàn, an ninh thông tin Trang thông tin điện tử (Website) của Cục, của Văn phòng thường trực Ban Chỉ đạo và hệ thống máy chủ, trang thiết bị CNTT đặt tại nhà A4 (số 02, Ngọc Hà); triển khai cài đặt phần mềm diệt Virus, phần mềm chống xâm nhập trái phép trên hệ thống máy chủ, máy tính cá nhân (máy tính công vụ) của công chức, viên chức, người lao động của Cục làm việc tại số 02, Ngọc Hà;

c) Tham mưu, bố trí lắp đặt máy tính, máy in, máy photocopy và các thiết bị CNTT khác (không kết nối mạng) để soạn thảo, lưu trữ thông tin, dữ liệu, tài liệu mật theo quy định của Luật Bảo vệ bí mật nhà nước.

2. Trách nhiệm của Phòng Thông tin, Truyền thông: tổ chức rà soát việc đảm bảo an toàn, an ninh thông tin các trang mạng xã hội (Facebook, Zalo, Viber,…) của Cục, của Văn phòng thường trực Ban Chỉ đạo.

3. Trách nhiệm của Phòng Kế hoạch, Tài chính:

a) Chủ trì nghiên cứu, hướng dẫn các đơn vị trực thuộc Cục áp dụng, vận dụng định mức kinh phí triển khai các nhiệm vụ, hoạt động về an toàn thông tin mạng và an ninh mạng theo quy định;

b) Tổng hợp, cân đối, tham mưu trình Cục trưởng bố trí kinh phí thực hiện nhiệm vụ đảm bảo an toàn thông tin mạng và an ninh mạng trong dự toán kinh phí hàng năm của Cục, của Văn phòng thường trực Ban Chỉ đạo.

4. Trách nhiệm của các phòng, Văn phòng đại diện Cục tại các khu vực chủ trì tham mưu, tổ chức triển khai, thực hiện và chịu trách nhiệm trước Cục trưởng về việc đảm bảo an toàn, an ninh thông tin đối với các hệ thống thông tin, CSDL do đơn vị xây dựng, quản lý, vận hành.

5. Trách nhiệm Trung tâm Chính sách và Kỹ thuật phòng, chống thiên tai:

a) Tổ chức rà soát, xây dựng hệ thống tường lửa, hệ thống máy chủ, hệ thống sao lưu dữ liệu, bảo đảm an toàn các hệ thống thông tin, CSDL do Trung tâm chủ trì xây dựng, triển khai và quản lý, vận hành;

b) Hỗ trợ kỹ thuật, hướng dẫn các đơn vị thuộc Cục triển khai, thực hiện các nhiệm vụ ứng dụng CNTT, chuyển đổi số của các đơn vị;

c) Phối hợp với Văn phòng Cục và các đơn vị có liên quan tham mưu, xây dựng hồ sơ cấp độ an toàn hệ thống thông tin trình cấp có thẩm quyền phê duyệt.

Điều 14. Điều khoản thi hành

1. Thủ trưởng các đơn vị trực thuộc Cục có trách nhiệm phổ biến, quán triệt đến toàn thể công chức, viên chức, người lao động trong đơn vị và chỉ đạo, tổ chức thực hiện Quy chế này.

2. Trong quá trình thực hiện, nếu có vướng mắc, phát sinh, các cơ quan, đơn vị, cá nhân kịp thời phản ánh về Văn phòng Cục để tổng hợp, báo cáo Cục trưởng xem xét sửa đổi, bổ sung Quy chế cho phù hợp./.

CỤC QUẢN LÝ ĐÊ ĐIỀU
VÀ PHÒNG, CHỐNG THIÊN TAI