BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG
CỤC LÂM NGHIỆP VÀ KIỂM LÂM

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

Số: 496 /QĐ-LNKL

Hà Nội, ngày 23 tháng 10 năm 2025

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Lâm nghiệp và Kiểm lâm

CỤC TRƯỞNG CỤC LÂM NGHIỆP VÀ KIỂM LÂM

Căn cứ Luật An toàn thông tin mạng năm 2015;

Căn cứ Luật An ninh mạng năm 2018;

Căn cứ Luật Bảo vệ bí mật nhà nước năm 2018;

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

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

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Căn cứ Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 138/QĐ-BNNMT ngày 01 tháng 3 năm 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 Lâm nghiệp và Kiểm lâm;

Căn cứ Quyết định số 1921/QĐ-BNNMT ngày 05 tháng 6 năm 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 Truyền thông và cơ sở dữ liệu Lâm nghiệp.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Lâm nghiệp và Kiểm lâm.

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

Điều 3. Chánh Văn phòng Cục; Trưởng phòng Truyền thông và Cơ sở dữ liệu lâm nghiệp; lãnh đạo các đơn vị thuộc, trực thuộc Cục; công chức, viên chức, người lao động Cục Lâm nghiệp và Kiểm lâm và tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Thứ trưởng Nguyễn Quốc Trị (để báo cáo);
- Cục Chuyển đổi số (để phối hợp);
- Lãnh đạo Cục (để báo cáo);
- Lưu: VT, TTDL.

CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC LÂM NGHIỆP VÀ KIỂM LÂM
BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG

Trần Quang Bảo

BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG
CỤC LÂM NGHIỆP VÀ KIỂM LÂM

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 TRONG HOẠT ĐỘNG ỨNG DỤNG CÔNG NGHỆ THÔNG TIN CỦA CÁC ĐƠN VỊ THUỘC CỤC LÂM NGHIỆP VÀ KIỂM LÂM

(Kèm theo Quyết định số /QĐ-LNKL ngày tháng năm 2025 của Cục trưởng Cục Lâm nghiệp và Kiểm lâm)

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, an ninh mạng trong các hoạt động Ứng dụng công nghệ thông tin của Cục Lâm nghiệp và Kiểm lâm (Sau đây gọi là Cục).

2. Đối tượng áp dụng

a) Các đơn vị thuộc, trực thuộc Cục Lâm nghiệp và Kiểm lâm (sau đây gọi là đơn vị thuộc, trực thuộc Cục) và công chức, viên chức, người lao động thuộc các đơn vị thuộc, trực thuộc Cục.

b) Cơ quan, tổ chức, cá nhân có sử dụng hoặc kết nối truy cập vào hệ thống mạng của Cục.

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin, an toàn thông tin mạng cho 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. *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.

3. *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…

4. *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.

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

6. 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.

7. 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.

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 phải gắn liền và hỗ trợ việc sử dụng thiết bị xử lý thông tin để xử lý công việc của công chức, viên chức, người lao động thuộc Cục.

4. 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.

5. 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

Thực hiện theo Điều 4 Quy chế bảo đảm an toàn, an ninh thông tin mạng Bộ Nông nghiệp và Môi trường tại 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.

Chương II
NỘI DUNG, BIỆN PHÁP BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 5. Lưu trữ và trao đổi thông tin

1. Việc lưu trữ và trao đổi thông tin phải tuân thủ các quy định của pháp luật về lưu trữ, CNTT và truyền thông.

2. Các dữ liệu, thông tin và tài liệu quan trọng, ở các mức độ mật, tối mật, tuyệt mật thì người sử dụng phải soạn thảo, lưu trữ tại máy tính soạn thảo văn bản bí mật nhà nước do Cục bố trí máy tính không kết nối mạng. Phải đặt mật khẩu, mã hóa dữ liệu và các biện pháp đảm bảo an toàn, an ninh thông tin, tuân thủ tuyệt đối nội quy Bảo vệ bí mật nhà nước và ANM được đặt tại phòng soạn thảo BMNN.

3. Các thiết bị kết nối mạng, thiết bị bảo mật quan trọng như tường lửa, thiết bị định tuyến, hệ thống máy chủ, hệ thống lưu trữ…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.

4. 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.

Điều 6. Yêu cầu về công tác bảo đảm an toàn thông tin

1. Đơn vị quản trị Công nghệ thông tin quản trị hệ thống mạng nội bộ của cơ quan Cục và hệ thống phải được trang bị hệ thống kỹ thuật, công nghệ hiện đại; thường xuyên được quản lý, giám sát, kiểm soát nhằm phát hiện và ngăn chặn các truy cập trái phép của người sử dụng và tin tặc.

2. Xây dựng hệ thống dự phòng cho các hệ thống CNTT cốt lõi như: máy chủ web, cơ sở dữ liệu, thư điện tử. Phải có quy trình phục hồi, sao lưu dữ liệu định kỳ cho hệ thống các phần mềm và cơ sở dữ liệu.

3. Quản lý chặt chẽ hệ thống tài khoản người sử dụng của các hệ thống thông tin, thư điện tử, và các tài nguyên mạng khác gồm các công việc: tạo mới, kích hoạt, sửa đổi, vô hiệu hoá, xoá bỏ,... Phải có biện pháp khóa hoặc hủy tài khoản, quyền truy nhập, thu hồi các thiết bị liên quan tới hệ thống thông tin (khóa, thẻ nhận dạng,...) cho phù hợp đối với công chức, viên chức đã nghỉ việc hoặc chuyển công tác.

4. Hệ thống thông tin quản lý, hệ thống cơ sở dữ liệu, hệ thống máy chủ phải có chức năng tự động ghi nhật ký (trong khoảng thời gian nhất định, tối thiểu là 3 tháng) quá trình đăng nhập vào hệ thống, các thao tác cấu hình hệ thống và các thông tin liên quan về ATTT để phục vụ công tác khắc phục sự cố và điều tra về ATTT khi xảy ra.

5. Việc tiêu huỷ thiết bị hoặc vật mang thông tin (đĩa cứng, đĩa di động,...) phải đảm bảo yêu cầu không để lộ, lọt thông tin nhà nước. Phải có quy trình cụ thể và phải lưu giữ hồ sơ, biên bản, tiêu huỷ.

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 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, trực 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. Một số biện pháp quản lý vận hành đảm bảo an toàn thông tin

1. Đơn vị sử dụng hệ thống

a) Bố trí công chức, viên chức tham gia phối hợp triển khai ATTT.

b) Máy tính bố trí cho các công chức, viên chức thực hiện nhiệm vụ được cài đặt ứng dụng văn phòng và phần mềm diệt virus có bản quyền. Người dùng sử dụng có trách nhiệm bảo quản, nghiêm cấm gỡ cài đặt các ứng dụng văn phòng và diệt virus đã được cài đặt. Thông tin cho bộ phận quản trị CNTT khi bản quyền hết hạn để cập nhật thông tin bản quyền kịp thời.

c) Người dùng phải đặt mật khẩu cho máy tính (mật khẩu đăng nhập, mật khẩu bảo vệ màn hình). Sử dụng các thiết bị lưu trữ thông tin (USB, ổ cứng gắn ngoài, thẻ nhớ,...) đảm bảo an toàn, đúng cách để phòng ngừa virus, phần mềm gián điệp xâm nhập máy tính phá hoại, đánh cắp thông tin. Định kỳ thường xuyên quét virus, phần mềm gián điệp trên máy tính.

2. Phòng Truyền thông và Cơ sở dữ liệu lâm nghiệp:

a) Tham mưu cho lãnh đạo Cục triển khai thực hiện các biện pháp để đảm bảo an toàn, an ninh hệ thống thông tin của cơ quan, đơn vị. Thường xuyên nghiên cứu, cập nhật các kiến thức về ATTT, có biện pháp phòng tránh các nguy cơ tiềm ẩn có thể gây mất thông tin khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ.

b) Thường xuyên cập nhật cấu hình chuẩn cho các thành phần của hệ thống thông tin, thiết lập cấu hình chặt chẽ nhất nhưng vẫn đảm bảo duy trì hoạt động thường xuyên của hệ thống thông tin.

c) Khi thiết lập cấu hình hệ thống thông tin cần xác định các chức năng, cổng giao tiếp mạng, giao thức và dịch vụ không cần thiết để cấm hoặc hạn chế sử dụng.

d) Thường xuyên thực hiện việc theo dõi bản ghi nhật ký hệ thống và các sự kiện khác có liên quan để đánh giá, báo cáo mức độ nghiêm trọng các rủi ro đó. Các rủi ro đó có thể xảy ra do sự truy cập trái phép, sử dụng trái phép, mất, thay đổi hoặc phá hủy thông tin và hệ thống thông tin.

đ) Kiểm soát chặt chẽ việc cài đặt phần mềm vào máy trạm và máy chủ.

Điều 9. Quản lý an toàn thông tin đối với hệ thống mạng nội bộ

1. Phải được thiết kế phân vùng theo chức năng cơ bản (theo các chính sách an toàn thông tin riêng), bao gồm nhưng không giới hạn các vùng mạng sau: 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.

2. 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 thông tin.

3. 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.

4. Thiết lập cấu hình chỉ cho phép kết nối mạng nội bộ sau khi các máy tính phục vụ công việc được đăng ký thông tin địa chỉ mạng vật lý (địa chỉ MAC).

5. 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.

6. Định kỳ thực hiện kiểm soát các phần mềm cài đặt, cập nhật, vá lỗi các điểm yếu bảo mật phần mềm, máy tính cá nhân, thiết bị kết nối mạng đang hoạt động thuộc hệ thống mạng nội bộ.

7. 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 cổng mạng không sử dụng.

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

Điều 10. Quản lý an toàn thông tin đối với kết nối internet

Hệ thống mạng của Cục phải 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:

1. 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.

2. Thiết lập mạng không dây riêng tách biệt với mạng nội bộ phục vụ cho các đối tác và người dùng vào mạng internet. Mật khẩu kết nối mạng không dây phải được thay đổi định kỳ tối thiểu 01 năm/lần, độ phức tạp trên 08 ký tự bao gồm tối

thiểu 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 : ; “ ‘ <> , . ? /).

3. Lọc bỏ, không cho phép truy nhập 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.

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

Điều 11. 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,...).

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.

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, Trung tâm Hạ tầng số 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.

5. Trường hợp cá nhân được cấp hoặc giao tài khoản 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 Phòng Truyền thông và Cơ sở dữ liệu lâm nghiệp để thực hiện việc điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng đối với tài khoản.

6. 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 12. Quản lý an toàn thông tin đối với dữ liệu

Thực hiện theo Điều 13 Quy chế bảo đảm an toàn, an ninh thông tin mạng Bộ Nông nghiệp và Môi trường tại Quyết định số 1921/QĐ-BNNMT ngày 05 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.

Điều 13. Quản lý an toàn thông tin đối với thiết bị số

1. Thiết bị số phục vụ quản trị hệ thống:

a) Phải cài đặt các phần mềm đảm bảo an toàn thông tin do Cục cung cấp, bao gồm nhưng không giới hạn: phần mềm chống mã độc tập trung, công cụ kết nối VPN.

b) Chỉ cài đặt và sử dụng các phần mềm quản trị đúng bản quyền, nguồn gốc rõ ràng, thực sự cần thiết.

2. Thiết bị số của các đơn vị thuộc Cục kết nối vào mạng nội bộ phải đáp ứng đầy đủ các yêu cầu sau:

a) Phải đăng ký với đơn vị chuyên trách an toàn thông tin của Cục các địa chỉ mạng vật lý (MAC).

b) Sử dụng hệ điều hành được hỗ trợ bản vá lỗ hổng bảo mật. Chỉ cài đặt tiện ích thiết yếu được cung cấp kèm theo hệ điều hành và các phần mềm phục vụ công việc, có bản quyền hoặc được các cơ quan chức năng đánh giá, xác nhận an toàn. Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; 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 chuyên trách về an toàn thông tin mạng để được xử lý kịp thời.

3. Thiết bị số soạn thảo văn bản chứa nội dung bí mật nhà nước, lưu trữ bí mật nhà nước:

a) Chỉ sử dụng máy tính bảo mật đã được quy định để soạn thảo và lưu trữ văn bản bí mật nhà nước. Không kết nối vào mạng Internet, mạng nội bộ, mạng không dây, mạng viễn thông.

b) Trường hợp thiết bị lưu trữ lỗi cần mang đi bảo hành, phải thực hiện biện pháp xóa dữ liệu vĩnh viễn trước khi mang ra khỏi cơ quan và có biên bản ghi nhận về việc xóa dữ liệu giữa đơn vị sử dụng máy tính và đơn vị nhận thiết bị lưu trữ. Việc sửa chữa, nâng cấp phần mềm cho máy tính (sau khi đã đưa vào sử dụng), nếu yêu cầu phải tiếp cận các tệp tin trên thiết bị lưu trữ, phải thực hiện dưới sự giám sát của đơn vị sử dụng thiết bị số, đảm bảo không lộ lọt dữ liệu trên thiết bị lưu trữ ra bên

ngoài trong quá trình này (có biên bản giữa đơn vị sử dụng thiết bị số và đơn vị sửa chữa, nâng cấp phần mềm).

4. Thiết bị lưu trữ di động cho các hoạt động nghiệp vụ, quản lý chỉ được sử dụng khi thực hiện các biện pháp bảo đảm an ninh, an toàn cho thiết bị như mã hóa dữ liệu, quét mã độc định kỳ.

Điều 14. Quản lý an toàn thông tin đối với 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 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.

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 15. Giám sát an toàn thông tin mạng

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

2. Giám sát và cấu hình cảnh báo các thay đổi trên các hệ thống; các hành vi cố gắng truy cập, đăng nhập thành công hoặc không thành công vào các hạ tầng quan trọng như hạ tầng ảo hóa, Domain Controller, VPN…

3. Thông báo cho các đầu mối ứng cứu sự cố của Bộ 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.

4. 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.

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

1. Phòng Truyền thông và Cơ sở dữ liệu lâm nghiệp có trách nhiệm theo dõi, nắm bắt thông tin trên phương tiện thông tin đại chúng và mạng Internet về các sự kiện mất an toàn thông tin mạng có thể tác động tới đơn vị; 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 Bộ (Cục chuyển đổi số) 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, an ninh thông tin mạng Bộ Nông nghiệp và Môi trường tại 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.

5. 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 Truyền thông và Cơ sở dữ liệu lâm nghiệp trong các hoạt động giám sát an toàn thông tin mạng tại đơn vị và tại Cục.

Điều 17. Phổ biến, tuyên truyền, đào tạo, bồi dưỡng về an toàn thông tin mạng

1. Phòng Truyền thông và Cơ sở dữ liệu lâm nghiệp 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 Truyền thông và Cơ sở dữ liệu lâm nghiệp phối hợp với Cục Chuyển đổi số 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.

Chương III
TRÁCH NHIỆM CỦA CÁC TỔ CHỨC, CÁ NHÂN LIÊN QUAN

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, trực thuộc Cục

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

2. Thực hiện việc quản lý trang thiết bị công nghệ thông tin và công chức, viên chức, người lao động theo Điều 10, Điều 11 và Điều 12 của Quy chế này.

3. 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.

4. 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. 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.

5. 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 Truyền thông và Cơ sở dữ liệu lâm nghiệp

1. Thực hiện trách nhiệm của đơn vị chuyên trách 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. Xây dựng kế hoạch, báo cáo về an toàn thông tin mạng của Cục.

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

4. Thường xuyên tổ chức các hoạt động tuyên truyền, phổ biến nâng cao nhận thức về an toàn thông tin mạng; nhận diện, cảnh giác, phòng ngừa và ngăn chặn các hoạt động vi phạm pháp luật trên không gian mạng tại Cục, Bộ lồng ghép trong các chương trình hội nghị, tập huấn, hội thảo về ứng dụng công nghệ thông tin.

5. 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.

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 cá nhân

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 chuyên 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 quan trọng hoặc dữ liệu mật của ngành nông nghiệp và môi trường do không tuân thủ Quy chế.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 23. Kinh phí thực hiện

Kinh phí bảo đảm an toàn thông tin mạng được lấy từ nguồn ngân sách nhà nước dự toán hàng năm của Cục Lâm nghiệp và Kiểm lâm theo quy định.

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 gửi Phòng kế hoạch - Tài chính để tổng hợp, thẩm định, trình cấp có thẩm quyền phê duyệt.

Điều 24. Chế độ báo cáo

1. Báo cáo định kỳ:

a) Báo cáo an toàn thông tin định kỳ hàng năm trước ngày 15 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 15 tháng 6 và 15 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 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 Truyền thông và Cơ sở dữ liệu lâm nghiệp.

b) Phòng Truyền thông và Cơ sở dữ liệu lâm nghiệp chịu trách nhiệm tập hợp, tổng hợp báo cáo của các đơn vị, trình Lãnh đạo Cục phê duyệt, gửi Lãnh đạo Bộ và các cơ quan quản lý nhà nước về an toàn thông tin.

Điều 25. 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 tình hình 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 26. 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 ảnh về Phòng Truyền thông và Cơ sở dữ liệu lâm nghiệp để tổng hợp, trình Cục trưởng xem xét, sửa đổi, bổ sung Quy chế cho phù hợp./.

CỤC LÂM NGHIỆP VÀ KIỂM LÂM