BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG
CỤC CHUYỂN ĐỔI SỐ

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

Số: 114 /QĐ-CĐS

Hà Nội, ngày 14 tháng 7 năm 2025

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Chuyển đổi số

CỤC TRƯỞNG CỤC CHUYỂN ĐỔI SỐ

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 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 223/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 Chuyển đổi số;

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 An toàn thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Chuyển đổi số.

Điều 2. Quyết định này có hiệu lực từ ngày ký và thay thế cho Quyết định số 194/QĐ-CĐS ngày 11 tháng 10 năm 2024 của Cục trưởng Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường Ban hành Quy chế bảo đảm an toàn thông tin mạng Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường.

Điều 3. Chánh Văn phòng Cục; Trưởng phòng An toàn thông tin; lãnh đạo các đơn vị trực thuộc Cục; công chức, viên chức, người lao động thuộc Cục Chuyển đổi số và tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Thứ trưởng Trần Quý Kiên (để báo cáo);
- Các đơn vị trực thuộc Bộ (để phối hợp);
- Cục trưởng Lê Phú Hà (để báo cáo);
- Các Phó Cục trưởng (để chỉ đạo);
- Các đơn vị trực thuộc Cục (để thực hiện);
- Lưu: VT, ATTT.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC CHUYỂN ĐỔI SỐ
BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG

Trần Văn Đoài

BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG
CỤC CHUYỂN ĐỔI SỐ

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 CỤC CHUYỂN ĐỔI SỐ

(Kèm theo Quyết định số /QĐ-CĐS ngày tháng năm 2025 của Cục trưởng Cục Chuyển đổi số)

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 bảo đảm an toàn thông tin mạng, an ninh mạng trong các hoạt động của Cục Chuyển đổi số (Sau đây gọi là Cục).

2. Đối tượng áp dụng

a) Các đơn vị trực thuộc Cục Chuyển đổi số (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) Cơ quan, tổ chức, cá nhân sử dụng dịch vụ công nghệ thông tin, an toàn thông tin mạng tại Trung tâm dữ liệu của Bộ do Cục quản lý.

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
QUY ĐỊNH BẢO ĐẢM AN TOÀN THÔNG TIN ĐỐI VỚI HẠ TẦNG CÔNG NGHỆ THÔNG TIN DÙNG CHUNG CỦA BỘ

Điều 5. Quản lý an toàn thông tin đối với Trung tâm dữ liệu

1. Trung tâm dữ liệu là khu vực hạn chế tiếp cận, chỉ những cá nhân có quyền, nhiệm vụ theo quy định của thủ trưởng cơ quan, đơn vị mới được phép vào Trung tâm dữ liệu. Quá trình vào, ra phải được ghi nhận vào nhật ký quản lý Trung tâm dữ liệu.

2. 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.

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.

5. Các đơn vị được giao quản trị, vận hành Trung tâm dữ liệu 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.

Điều 6. Quản lý an toàn thông tin đối với hệ thống máy chủ và ứng dụng đặt tại Trung tâm dữ liệu

1. Phải được đặt trong các vùng mạng dành riêng cho máy chủ, tối thiểu gồm vùng mạng máy chủ công cộng, vùng mạng máy chủ nội bộ, vùng mạng máy chủ cơ sở dữ liệu, và vùng quản trị.

2. 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.

3. 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.

4. 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 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.

5. 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.

6. 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.

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

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

b) 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.

c) 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.

d) 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.

đ) 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.

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 thiếp 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.

Chương III
QUY ĐỊNH BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG NỘI BỘ DO CỤC QUẢN LÝ

Điều 8. 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 9. 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 10. 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. 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 11. 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 12. 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) Sử dụng hệ điều hành và các phần mềm soạn thảo văn bản có bản quyền. 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 13. 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 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 14. Giám sát an toàn thông tin mạng

1. Giao Trung tâm Hạ tầng số 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. 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 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.

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

1. Phòng An toàn thông tin có thẩm quyền yêu cầu kiểm tra, đánh giá đối với các hệ thống thông tin.