Ký bởi: CỤC CHUYỂN ĐỔI SỐ
Email: cuccds@mae.gov.vn
Cơ quan: BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG
Ngày ký: 05-10-2026 11:02:01 +07:00

BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG

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

Số: 3785/QĐ-BNNMT

Hà Nội, ngày 05 tháng 10 năm 2026

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an ninh mạng Bộ Nông nghiệp và Môi trường

BỘ TRƯỞNG BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG

Căn cứ Luật Dữ liệu ngày 30 tháng 11 năm 2024;

Căn cứ Luật Bảo vệ dữ liệu cá nhân ngày 26 tháng 6 năm 2025;

Căn cứ Luật Bảo vệ bí mật nhà nước ngày 10 tháng 12 năm 2025;

Căn cứ Luật An ninh mạng ngày 10 tháng 12 năm 2025;

Căn cứ Nghị định số 355/2026/NĐ-CP ngày 11 tháng 9 năm 2026 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Nông nghiệp và Môi trường;

Căn cứ Nghị định số 356/2025/NĐ-CP ngày 31 tháng 12 năm 2025 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân;

Căn cứ Nghị định số 327/2026/NĐ-CP ngày 19 tháng 8 năm 2026 của Chính phủ quy định về phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng;

Căn cứ Nghị định số 328/2026/NĐ-CP ngày 19 tháng 8 năm 2026 của Chính phủ quy định phòng, chống tin giả, tin sai sự thật;

Căn cứ Nghị định số 329/2026/NĐ-CP ngày 19 tháng 8 năm 2026 của Chính phủ quy định về lực lượng bảo vệ an ninh mạng;

Căn cứ Nghị định số 330/2026/NĐ-CP ngày 19 tháng 8 năm 2026 của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực an ninh mạng và bảo vệ dữ liệu cá nhân;

Căn cứ Nghị định số 331/2026/NĐ-CP ngày 19 tháng 8 năm 2026 của Chính phủ về bảo vệ an ninh mạng đối với hệ thống thông tin;

Căn cứ Nghị định số 332/2026/NĐ-CP ngày 19 tháng 8 năm 2026 của Chính phủ quy định về hoạt động kinh doanh sản phẩm, dịch vụ an ninh mạng;

Căn cứ Nghị định số 333/2026/NĐ-CP ngày 19 tháng 8 năm 2026 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật An ninh mạng;

Căn cứ Quy chuẩn kỹ thuật quốc gia QCVN 12:2026/BCA An ninh mạng cho hệ thống thông tin lưu trữ tài liệu điện tử trong các cơ quan đảng, Nhà nước;

Căn cứ Tiêu chuẩn quốc gia TCVN 14423:2026 về An ninh mạng - Yêu cầu đối với hệ thống thông tin quan trọng;

Theo đề nghị của Cục trưởng Cục Chuyển đổi số.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an ninh mạng Bộ Nông nghiệp và Môi trường.

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

Điều 3. Chánh Văn phòng Bộ; Cục trưởng Cục Chuyển đổi số; Thủ trưởng các đơn vị trực thuộc Bộ Nông nghiệp và Môi trường; công chức, viên chức, người lao động thuộc Bộ Nông nghiệp và Môi trường và tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Văn phòng Chính phủ;
- Bộ Công an;
- Bộ Quốc phòng;
- Bộ Khoa học và Công nghệ;
- Ban Cơ yếu Chính phủ;
- Bộ trưởng (để báo cáo);
- Các Thứ trưởng;
- Sở NN và MT các tỉnh, thành phố;
- Cổng thông tin điện tử Bộ;
- Lưu: VT, CĐS.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG

Đặng Ngọc Điệp

BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG

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

QUY CHẾ
BẢO ĐẢM AN NINH MẠNG BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG

(Kèm theo Quyết định số /QĐ-BNNMT ngày tháng năm 2026 của Bộ trưởng Bộ Nông nghiệp và Môi trường)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh: Quy chế này quy định về công tác bảo đảm an ninh mạng trong các hoạt động của Bộ Nông nghiệp và Môi trường (sau đây gọi tắt là Bộ).

2. Đối tượng áp dụng

a) Các đơn vị trực thuộc Bộ Nông nghiệp và Môi trường (sau đây gọi là đơn vị trực thuộc Bộ); công chức, viên chức và người lao động thuộc các đơn vị trực thuộc Bộ;

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

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin, an ninh mạng cho các đơn vị trực thuộc Bộ.

Điều 2. Giải thích từ ngữ

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

1. *An ninh mạng* là sự ổn định, an ninh, an toàn của không gian mạng; bảo vệ hệ thống thông tin và bảo đảm thông tin, dữ liệu, 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.

2. *An ninh thông tin mạng* là sự bảo đảm tính nguyên vẹn, tính bảo mật, tính khả dụng của thông tin trên không gian mạng, tránh bị truy cập, sử dụng, tiết lộ, sửa đổi trái phép, phá hoại hoặc hành vi khác đe dọa hoặc gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội.

3. *An ninh dữ liệu* là sự bảo đảm chất lượng dữ liệu và các hoạt động xử lý, sử dụng dữ liệu trên không gian mạng phục vụ phát triển kinh tế - xã hội, chuyển đổi số quốc gia, tránh bị truy cập, sử dụng, tiết lộ, sửa đổi trái phép, phá hoại hoặc hành vi khác đe dọa hoặc gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội.

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. *Cổng thông tin điện tử* là điểm truy cập duy nhất của cơ quan, đơn vị trên môi trường mạng, liên kết, tích hợp các kênh thông tin, các dịch vụ và các ứng dụng mà qua đó người dùng có thể khai thác, sử dụng và cá nhân hóa việc hiển thị thông tin.

7. *Trang thông tin điện tử* là hệ thống thông tin dùng để thiết lập một hoặc nhiều trang thông tin 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 và sử dụng thông tin trên Internet.

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

9. *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.

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

11. *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.

12. *Sự cố an ninh mạng* là sự việc bất ngờ xảy ra trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

13. Rủi ro an ninh mạng là khả năng bị lộ hoặc mất mát do một cuộc tấn công mạng hoặc vi phạm dữ liệu trong cơ quan, tổ chức, đơn vị. Rủi ro an ninh mạng không chỉ nằm ở khả năng xảy ra một cuộc tấn công mạng mà còn là những hậu quả tiềm ẩn, ví dụ như tổn thất tài chính, thiệt hại về danh tiếng hoặc gián đoạn hoạt động.

14. *Tài khoản số* là thông tin dùng để chứng thực, xác thực, phân quyền sử dụng các ứng dụng, dịch vụ trên không gian mạng.

15. *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.

16. *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 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. Các hành vi bị nghiêm cấm

1. Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật An ninh mạng, Điều 7 Luật Bảo vệ dữ liệu cá nhân, Điều 10 của Luật Dữ liệu 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 ninh mạng 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, tổ chức, 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 gây nguy cơ đe dọa an ninh mạng, làm tổn hại, lọt, lộ bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

Chương II
QUY ĐỊNH BẢO ĐẢM AN NINH MẠNG

Điều 4. Nguyên tắc bảo đảm an ninh mạng

1. Bảo đảm an ninh mạng là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt quá trình liên quan đến thông tin và thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ hệ thống thông tin. Bảo đảm an ninh mạng tuân thủ các nguyên tắc chung quy định tại Điều 4 của Luật An ninh mạng và Điều 6 của Nghị định 331/2026/NĐ-CP và các quy định pháp luật khác có liên quan.

2. Tuân thủ các quy định và hướng dẫn về bảo đảm an ninh mạng của cơ quan có thẩm quyền. Trường hợp có văn bản, quy định cập nhật, thay thế hoặc quy định

khác tại văn bản quy phạm pháp luật, quyết định của cấp có thẩm quyền cao hơn thì áp dụng quy định tại văn bản đó.

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

4. Việc bảo đảm an ninh mạng cho hệ thống thông tin được thực hiện một cách tổng thể, đồng bộ, tập trung trong việc đầu tư các giải pháp bảo vệ, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp. Các nhiệm vụ, dự án chuyển đổi số, ứng dụng công nghệ thông tin hoặc có cấu phần công nghệ thông tin quy định tại khoản 1 và khoản 2 Điều 1 của Nghị định số 45/2026/NĐ-CP phải có ý kiến thẩm định nội dung liên quan đến an ninh mạng, phê duyệt hồ sơ cấp độ và phương án bảo đảm an toàn hệ thống thông tin theo cấp độ trước khi được phê duyệt.

5. Quản lý, sử dụng và bảo đảm an ninh mạng, mạng máy tính nội bộ có lưu trữ, truyền đưa bí mật nhà nước phải được tách biệt vật lý hoàn toàn với mạng máy tính, các thiết bị, phương tiện điện tử có kết nối mạng Internet, trường hợp truyền nhận thông tin qua Hệ thống quản lý văn bản và Hồ sơ công việc mật của Chính phủ phải sử dụng các thiết bị mã hóa và đường truyền chuyên dụng do Ban Cơ yếu Chính phủ cung cấp và xác thực.

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

7. Các hệ thống thông tin dùng chung của Bộ và của các đơn vị trực thuộc Bộ phải được phê duyệt hồ sơ đề xuất cấp độ và có phương án bảo đảm an ninh mạng tương ứng với cấp độ trước khi đưa vào sử dụng.

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

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

1. Chủ quản hệ thống thông tin

a) Bộ Nông nghiệp và Môi trường là chủ quản hệ thống thông tin đối với các hệ thống thông tin do Bộ quyết định đầu tư hoặc Bộ được giao làm chủ đầu tư các nhiệm vụ, dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin. Bộ Nông nghiệp và Môi trường ủy quyền cho các đơn vị thuộc Bộ quản lý trực tiếp các hệ thống thông tin do Bộ làm chủ quản;

b) Các đơn vị thuộc Bộ là chủ quản hệ thống thông tin do đơn vị quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin; là chủ quản hệ thống thông tin do đơn vị phê duyệt đề cương, dự toán chi tiết; quản lý trực tiếp các hệ thống thông tin do Bộ ủy quyền theo quy định tại điểm a khoản này;

c) Chủ quản hệ thống thông tin (hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin) quy định tại Điều 4 của Nghị định số 331/2026/NĐ-CP.

2. Đơn vị vận hành hệ thống thông tin

a) Các hệ thống thông tin trước khi đưa vào khai thác, sử dụng phải được giao cho đơn vị quản lý, vận hành;

b) Giao Cục Chuyển đổi số là đơn vị vận hành các hệ thống thông tin, cơ sở dữ liệu dùng chung của Bộ và các hệ thống thông tin do Văn phòng Bộ, các Vụ trực thuộc Bộ quản lý sử dụng;

c) Đơn vị vận hành hệ thống thông tin được xác định theo Điều 5 của Nghị định số 331/2026/NĐ-CP;

3. Đơn vị chuyên trách về an ninh mạng

a) Cục Chuyển đổi số là đơn vị chuyên trách về an ninh mạng của Bộ;

b) Đơn vị hoặc bộ phận được giao thực hiện nhiệm vụ công nghệ thông tin, chuyển đổi số tại các đơn vị trực thuộc Bộ là đầu mối tham mưu, tổ chức thực hiện nhiệm vụ về an ninh mạng tại đơn vị.

Điều 6. Trình tự, thủ tục, thẩm quyền xác định cấp độ hệ thống thông tin

1. Đơn vị lập hồ sơ đề xuất cấp độ

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

2. Hồ sơ đề xuất cấp độ, nội dung Thuyết minh hồ sơ đề xuất cấp độ hệ thống thông tin quy định tại Điều 21 và Điều 22 Nghị định số 331/2026/NĐ-CP.

3. Xác định cấp độ đối với dự án đầu tư xây dựng mới hoặc mở rộng, nâng cấp hệ thống thông tin được quy định tại Điều 19 Nghị định số 331/2026/NĐ-CP.

4. Trình tự, thủ tục xác định cấp độ đối với hệ thống thông tin đang vận hành được quy định tại Điều 20 Nghị định số 331/2026/NĐ-CP.

5. Thẩm quyền thẩm định và phê duyệt cấp độ được quy định tại Điều 18 Nghị định số 331/2026/NĐ-CP.

Điều 7. Phương án bảo đảm an ninh mạng cho hệ thống thông tin

1. Phương án bảo đảm an ninh mạng cho hệ thống thông tin đối với từng cấp độ phải đáp ứng yêu cầu quy định tại Điều 29, Điều 30 Nghị định số 331/2026/NĐ-CP, phù hợp với tiêu chuẩn TCVN 11930:2017, TCVN 14423:2026, QCVN 12:2026/BCA và các văn bản quy phạm pháp luật, tiêu chuẩn, quy chuẩn kỹ thuật sửa đổi, bổ sung hoặc thay thế (nếu có).

2. Chủ quản hệ thống thông tin hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin tổ chức triển khai phương án bảo đảm an ninh mạng cho hệ thống thông tin sau khi hồ sơ đề xuất cấp độ và phương án bảo đảm an ninh mạng tương ứng được phê duyệt.

3. Đơn vị/bộ phận chuyên trách về an ninh mạng thuộc đơn vị chịu trách nhiệm giám sát việc triển khai các phương án bảo đảm an ninh mạng đã được phê duyệt.

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

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

1. Khi thực hiện nâng cấp, mở rộng, thay thế một phần hệ thống thông tin, phải rà soát cấp độ, phương án bảo đảm an ninh mạng 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 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. Các hệ thống thông tin được cài đặt tại Trung tâm dữ liệu của Bộ cần đáp ứng các yêu cầu:

a) Tách biệt với các môi trường phát triển, kiểm tra và thử nghiệm;

b) Áp dụng các giải pháp bảo đảm an ninh mạng;

c) Không cài đặt các công cụ, phương tiện phát triển ứng dụng;

d) Loại bỏ hoặc tắt các tính năng, phần mềm tiện ích không sử dụng trên hệ thống thông tin;

đ) Áp dụng các biện pháp bảo đảm tính toàn vẹn dữ liệu;

e) Mọi thao tác trên hệ thống phải được lưu vết, sẵn sàng cho kiểm tra, kiểm soát khi cần thiết.

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 ninh mạng cho hệ thống thông tin đáp ứng yêu cầu cơ bản trong tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm an ninh mạng 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 Bộ 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 ninh mạng, 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 9. Quản lý an ninh mạng về vật lý đối với trung tâm dữ liệu, phòng máy chủ

1. Trung tâm dữ liệu/phòng máy chủ

a) 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/phòng máy chủ. Quá trình vào, ra trung tâm dữ liệu/phòng máy chủ phải được ghi nhận vào nhật ký quản lý;

b) Phải được trang bị hệ thống lưu điện đủ công suất và duy trì thời gian hoạt động của các máy chủ ít nhất 15 phút khi có sự cố mất điện;

c) 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;

d) Đơn vị chủ quản trung tâm dữ liệu/phòng máy chủ có trách nhiệm xây dựng nội quy hoặc hướng dẫn làm việc tại khu vực này; phải cử cán bộ thường xuyên giám sát thiết bị, hạ tầng của trung tâm dữ liệu/phòng máy chủ.

2. 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…

a) Phải được đặt trong trung tâm dữ liệu/phòng máy chủ;

b) Phải được thiết lập cơ chế bảo vệ, theo dõi phát hiện xâm nhập và biện pháp kiểm soát truy cập, 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.

Điều 10. Quản lý an ninh mạng đối với hạ tầng mạng, hệ thống máy chủ và thiết bị số

1. Hạ tầng mạng

a) Hệ thống mạng nội bộ

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

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

- Thiết lập, cấu hình các tính năng theo thiết kế của các trang thiết bị bảo mật mạng; thực hiện các biện pháp, giải pháp để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng về mặt kỹ thuật của hệ thống mạng; thường xuyên kiểm tra, phát hiện những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào mạng;

- Định kỳ sao lưu cấu hình thiết bị kết nối mạng nội bộ. Lưu trữ tối thiểu trong 12 tháng đối với nhật ký của các thiết bị mạng và bảo đảm đồng bộ thời gian nhật ký với máy chủ thời gian thực theo múi giờ Việt Nam;

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

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

b) Kết nối mạng Internet

Các đơn vị trực thuộc Bộ phải áp dụng các biện pháp kỹ thuật cần thiết bảo đảm an ninh mạng trong kết nối vào Internet, tối thiểu đáp ứng các yêu cầu sau:

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

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

c) Các đơn vị khi có nhu cầu kết nối trang thiết bị vào hệ thống mạng máy tính của Bộ Nông nghiệp và Môi trường với mục đích phục vụ công việc, có trách nhiệm thông báo bằng công văn cho Cục Chuyển đổi số để phối hợp thực hiện việc kết nối vào mạng máy tính của Bộ;

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

đ) Các cơ quan bên ngoài khi có kết nối trực tiếp vào mạng của Bộ Nông nghiệp và Môi trường phải được sự đồng ý bằng văn bản của Cục Chuyển đổi số và tuân thủ các quy định, các tiêu chuẩn kỹ thuật.

2. Hệ thống máy chủ

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

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

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

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

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

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

g) Giám sát thường xuyên, liên tục để phát hiện và cảnh báo sớm nguy cơ đe dọa an ninh mạng.

3. Thiết bị số

a) Người sử dụng chỉ cài đặt phần mềm có hỗ trợ cập nhật các bản vá, tính năng mới, bản vá lỗ hổng bảo mật; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của bộ phận chuyên trách về công nghệ thông tin; thường xuyên cập nhật bản vá cho các phần mềm ứng dụng, hệ điều hành và các phần mềm phục vụ công việc;

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

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

d) Khóa màn hình máy tính khi rời khỏi bàn làm việc; đăng xuất khỏi hệ thống, ứng dụng khi ngừng sử dụng; tắt máy an toàn sau mỗi buổi làm việc. Các máy tính người dùng phải được cấu hình tự động khóa phiên làm việc hoặc kích hoạt chế độ khóa màn hình sau tối đa 15 phút không có hoạt động; các tài khoản, phiên làm việc quản trị hệ thống phải được tự động khóa hoặc yêu cầu xác thực lại sau tối đa 05 phút không có hoạt động;

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

e) Báo cáo và phải được thủ trưởng cơ quan, đơn vị đồng ý, cho phép trước khi mang thiết bị số thuộc sở hữu riêng đến nơi làm việc và kết nối với mạng nội bộ để xử lý công việc;

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

4. Bảo đảm an ninh mạng cho thiết bị camera giám sát

a) Thiết bị camera giám sát phải được quản lý trong mạng nội bộ riêng biệt, có biện pháp bảo mật khi kết nối Internet.

b) Dữ liệu hình ảnh thu được từ camera giám sát phải được mã hóa trong quá trình truyền và lưu trữ, đồng thời có chính sách phân quyền truy cập rõ ràng.

c) Nghiêm cấm sử dụng thiết bị camera giám sát không rõ nguồn gốc, không đạt chuẩn kỹ thuật an ninh mạng theo QCVN 11:2026/BCA.

d) Đơn vị chủ quản hệ thống camera giám sát phải định kỳ kiểm tra, đánh giá an toàn thiết bị và báo cáo về Cục Chuyển đổi số.

Điều 11. Quản lý an ninh mạng đối với tài khoản truy cập

1. Người sử dụng truy cập vào các hệ thống thông tin được cấp và sử dụng tài khoản truy cập với định danh duy nhất gắn với cá nhân đó. Các hệ thống thông tin dùng chung của Bộ sử dụng cơ chế đăng nhập một lần, mỗi người sử dụng một tài khoản định danh duy nhất; không sử dụng chung tài khoản hoặc mật khẩu.

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

3. Tài khoản quản trị hệ thống (mạng, hệ điều hành, thiết bị kết nối mạng, phần mềm, ứng dụng, cơ sở dữ liệu) phải tách biệt với tài khoản truy cập của người sử dụng thông thường. Tài khoản hệ thống phải được giao đích danh cá nhân làm công tác quản trị. Không sử dụng chung tài khoản quản trị, trừ trường hợp đặc biệt được cấp có thẩm quyền phê duyệt và có biện pháp kiểm soát, ghi nhật ký đầy đủ.

4. Hệ thống thông tin phải hỗ trợ khóa, thu hồi hoặc vô hiệu hóa tài khoản khi phát hiện dấu hiệu mất an toàn, an ninh mạng hoặc theo yêu cầu của chủ quản hệ thống thông tin. Tài khoản không phát sinh hoạt động trong thời gian liên tục từ 45 ngày trở lên phải được vô hiệu hóa hoặc chuyển sang trạng thái khóa để xem xét kích hoạt lại khi có nhu cầu sử dụng.

5. Quy định về đặt mật khẩu cho tài khoản truy cập của người sử dụng phải đáp ứng các yêu cầu sau:

a) Mật khẩu của tài khoản người sử dụng phải có tối thiểu 10 ký tự; mật khẩu của tài khoản quản trị phải có tối thiểu 12 ký tự và bao gồm ít nhất 03 trong 04 nhóm ký tự: chữ hoa, chữ thường, chữ số và ký tự đặc biệt;

b) Mật khẩu không được chứa tên tài khoản, thông tin dễ đoán hoặc thông tin liên quan trực tiếp đến người sử dụng;

c) Mật khẩu phải được thay đổi ngay khi tài khoản được cấp, kích hoạt hoặc bàn giao quyền quản trị, khi có nghi ngờ bị lộ hoặc khi có cảnh báo, sự cố an ninh mạng liên quan đến khả năng lộ lọt thông tin xác thực;

d) Mật khẩu của tài khoản người sử dụng phải được thay đổi tối thiểu 12 tháng một lần; mật khẩu của tài khoản quản trị phải được thay đổi tối thiểu 02 tháng một lần.

6. Bắt buộc áp dụng xác thực đa nhân tố (Multi-Factor Authentication - MFA) đối với các trường hợp sau:

a) Tất cả các tài khoản có quyền quản trị hệ thống, bao gồm nhưng không giới hạn ở tài khoản quản trị hệ điều hành, máy chủ, thiết bị mạng, thiết bị bảo mật, cơ sở dữ liệu, ứng dụng và các hệ thống thông tin khác;

b) Các phiên truy cập từ mạng bên ngoài, từ Internet hoặc từ các tổ chức, cá nhân bên thứ ba vào hệ thống thông tin thuộc phạm vi quản lý của Bộ;

c) Các tài khoản truy cập từ xa hoặc truy cập đến các hệ thống thông tin xử lý, lưu trữ dữ liệu quan trọng, dữ liệu nhạy cảm theo quy định của pháp luật và của Bộ.

Trường hợp hệ thống thông tin hoặc dịch vụ chưa hỗ trợ xác thực đa nhân tố, chủ quản hệ thống phải áp dụng các biện pháp kiểm soát tăng cường để giảm thiểu rủi ro, bao gồm giới hạn phạm vi truy cập, giới hạn địa chỉ IP nguồn, sử dụng mạng riêng ảo (VPN), tăng cường giám sát nhật ký truy cập, áp dụng chính sách mật khẩu mạnh và các biện pháp bảo vệ tương đương khác; đồng thời xây dựng kế hoạch, lộ trình triển khai xác thực đa nhân tố và hoàn thành trong thời gian sớm nhất. Việc duy trì các tài khoản hoặc dịch vụ thuộc đối tượng bắt buộc áp dụng MFA nhưng chưa triển khai MFA phải được đánh giá rủi ro, phê duyệt bằng văn bản của chủ quản hệ thống và chịu sự giám sát của đơn vị chuyên trách về an ninh mạng.

7. Người sử dụng và người làm công tác quản trị hệ thống có trách nhiệm bảo vệ thông tin xác thực được cấp; không tiết lộ, chia sẻ mật khẩu, thiết bị hoặc phương tiện xác thực cho người khác, trừ trường hợp bàn giao, cung cấp theo yêu cầu của cơ quan có thẩm quyền hoặc để phục vụ công tác quản lý, vận hành theo quy định của đơn vị.

Điều 12. Quản lý an ninh mạng đối với ứng dụng

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

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

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

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

5. Ghi và lưu giữ bản ghi nhật ký hệ thống (log files) của phần mềm, ứng dụng trong khoảng thời gian tối thiểu 12 tháng theo quy định.

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

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

Điều 13. Quản lý an ninh mạng đối với dữ liệu

1. Các đơn vị có trách nhiệm bảo vệ thông tin, dữ liệu trong toàn bộ vòng đời từ khởi tạo, thu thập, xử lý, lưu trữ, chia sẻ, truyền đưa, sao lưu đến tiêu hủy; bảo đảm tính bí mật, toàn vẹn, khả dụng và khả năng truy vết của dữ liệu theo quy định của pháp luật.

2. Thông tin, dữ liệu phải được phân loại và gán nhãn mức độ nhạy cảm để áp dụng các biện pháp quản lý, bảo vệ phù hợp. Tối thiểu áp dụng các mức phân loại sau:

a) Công khai;

b) Nội bộ;

c) Hạn chế truy cập;

d) Bí mật.

Việc phân loại, gán nhãn, quản lý, chia sẻ và lưu trữ dữ liệu phải phù hợp với mức độ nhạy cảm của dữ liệu và các quy định của pháp luật về bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân và các quy định có liên quan.

3. Dữ liệu quan trọng, dữ liệu nhạy cảm, dữ liệu cá nhân và dữ liệu phục vụ hoạt động của hệ thống thông tin phải được bảo vệ bằng các biện pháp kỹ thuật phù hợp, bao gồm mã hóa khi lưu trữ và truyền tải, kiểm soát truy cập, xác thực người sử dụng, ghi nhật ký và các biện pháp bảo vệ khác theo quy định.

4. Các đơn vị phải triển khai hệ thống hoặc phương tiện lưu trữ độc lập để thực hiện sao lưu dữ liệu dự phòng. Dữ liệu sao lưu tối thiểu bao gồm: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu, dữ liệu nghiệp vụ và các dữ liệu quan trọng khác của hệ thống thông tin.

5. Việc sao lưu dữ liệu phải tuân thủ nguyên tắc tối thiểu:

a) Duy trì ít nhất 03 bản sao dữ liệu, bao gồm dữ liệu gốc và các bản sao lưu;

b) Lưu trữ trên tối thiểu 02 loại phương tiện hoặc hệ thống lưu trữ khác nhau;

c) Có ít nhất 01 bản sao lưu được cách ly vật lý hoặc cách ly logic với hệ thống khai thác chính (air-gap hoặc giải pháp tương đương) để phòng chống mất mát dữ liệu do mã độc, tấn công mạng hoặc sự cố hệ thống;

d) Định kỳ kiểm tra khả năng khôi phục dữ liệu từ các bản sao lưu và lưu giữ hồ sơ kiểm tra theo quy định.

6. Trang thiết bị công nghệ thông tin có lưu trữ dữ liệu nhạy cảm khi thay đổi mục đích sử dụng, bảo hành, bảo dưỡng, sửa chữa, điều chuyển hoặc thanh lý phải được thực hiện các biện pháp xóa, hủy hoặc tiêu hủy dữ liệu bảo đảm không thể phục hồi. Trường hợp không thể xóa dữ liệu an toàn thì phải tháo rời hoặc tiêu hủy vật lý thiết bị lưu trữ theo quy định.

7. Việc soạn thảo, xử lý, lưu trữ và trao đổi thông tin thuộc phạm vi bí mật nhà nước phải tuân thủ quy định của pháp luật về bảo vệ bí mật nhà nước. Thiết bị chứa thông tin mật không được kết nối mạng, trừ trường hợp được phép theo quy định của cơ quan có thẩm quyền và áp dụng các giải pháp bảo mật được cơ quan có thẩm quyền đánh giá, chấp thuận.

8. Các đơn vị trực thuộc Bộ có trách nhiệm kiểm tra, giám sát các hoạt động chia sẻ, gửi, nhận thông tin, dữ liệu; áp dụng các biện pháp bảo vệ phù hợp đối với dữ liệu được trao đổi trên môi trường mạng, bao gồm mã hóa, đặt mật khẩu bảo vệ tệp tin, xác thực người sử dụng và các biện pháp kỹ thuật cần thiết khác.

9. Việc trao đổi, cung cấp hoặc chia sẻ thông tin, dữ liệu với cơ quan, tổ chức, cá nhân bên ngoài phải được kiểm soát, ghi nhận và áp dụng các biện pháp bảo vệ phù hợp với mức độ nhạy cảm của dữ liệu; sử dụng các giao thức truyền thông an toàn, cơ chế xác thực mạnh và chữ ký số theo quy định.

Điều 14. Quản lý an ninh mạng đối với công chức, viên chức và người lao động

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

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

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

2. Quy định trách nhiệm bảo đảm an ninh mạng trong quản lý và sử dụng nhân sự

Các đơn vị trực thuộc Bộ có trách nhiệm:

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

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

c) Đối với các vị trí tiếp xúc, quản lý các thông tin, dữ liệu quan trọng hoặc quản trị các hệ thống thông tin quan trọng, đơn vị phải yêu cầu nhân sự mới cam kết bảo mật thông tin bằng văn bản hoặc cam kết trong hợp đồng làm việc, hợp đồng

lao động, bao gồm các điều khoản về trách nhiệm của cá nhân sau khi thôi việc tại đơn vị;

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

đ) 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 công chức, viên chức và người lao động bảo đảm quyền truy cập phù hợp với nhiệm vụ được giao.

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

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

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

c) Thay đổi hoặc thu hồi quyền truy cập các hệ thống thông tin;

d) Rà soát, kiểm tra đối chiếu định kỳ giữa bộ phận quản lý nhân sự và bộ phận quản lý cấp phát, thu hồi quyền truy cập 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. Quản lý rủi ro an ninh mạng

1. Các đơn vị trực thuộc Bộ phải định kỳ thực hiện tối thiểu 01 lần/năm đánh giá rủi ro an ninh mạng đối với hệ thống thông tin theo cấp độ đã được phê duyệt.

2. Việc đánh giá rủi ro phải bao gồm: nhận diện mối đe dọa, phân tích điểm yếu, xác định khả năng xảy ra và mức độ tác động.

3. Kết quả đánh giá rủi ro phải được báo cáo về Cục Chuyển đổi số để tổng hợp, theo dõi và đề xuất biện pháp phòng ngừa, khắc phục.

Điều 16. Giám sát an ninh mạng

1. Các hệ thống thông tin thuộc phạm vi quản lý của Bộ phải được triển khai giám sát an ninh mạng theo quy định của pháp luật.

2. Chủ quản hệ thống thông tin có trách nhiệm tổ chức, chỉ đạo hoạt động giám sát an ninh mạng đối với các hệ thống thông tin thuộc phạm vi quản lý; phối hợp với Cục Chuyển đổi số và các cơ quan, đơn vị có liên quan trong việc giám sát, tiếp nhận, xử lý cảnh báo, cung cấp, trao đổi và chia sẻ thông tin phục vụ phát hiện, cảnh báo và xử lý các nguy cơ, sự cố mất an toàn, an ninh mạng.

3. Các hệ thống thông tin phải triển khai chức năng ghi, thu thập và lưu trữ nhật ký phục vụ công tác giám sát an ninh mạng theo quy định tại Điều 10, Điều 12 của Quy chế này.

4. Đối với hệ thống thông tin quan trọng về an ninh quốc gia, Chủ quản hệ thống thông tin có trách nhiệm phối hợp với cơ quan có thẩm quyền triển khai giám sát an ninh mạng theo quy định của pháp luật.

Điều 17. Kiểm tra, đánh giá an ninh mạng

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

2. Chủ quản hệ thống thông tin có thẩm quyền yêu cầu kiểm tra, đánh giá an ninh mạng đối với các hệ thống thông tin thuộc phạm vi quản lý. Đơn vị chuyên trách về an ninh mạng của chủ quản hệ thống thông tin có thẩm quyền yêu cầu kiểm tra, đánh giá đối với các hệ thống thông tin do đơn vị này thẩm định hồ sơ đề xuất cấp độ.

3. Đơn vị chủ trì kiểm tra, đánh giá là đơn vị được cấp có thẩm quyền giao nhiệm vụ hoặc được lựa chọn để thực hiện việc kiểm tra, đánh giá. Đối tượng kiểm tra, đánh giá là chủ quản hệ thống thông tin hoặc đơn vị vận hành hệ thống thông tin và các hệ thống thông tin có liên quan.

4. Cục Chuyển đổi số thực hiện kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an ninh mạng cho hệ thống thông tin theo cấp độ tại Bộ Nông nghiệp và Môi trường.

5. Cục Chuyển đổi số, đơn vị chuyên trách về an ninh mạng của các đơn vị trực thuộc Bộ thực hiện việc đánh giá hiệu quả các biện pháp bảo đảm an ninh mạng theo thẩm quyền.

Điều 18. Ứng cứu sự cố an ninh mạng

1. Cơ quan thường trực ứng cứu sự cố an ninh mạng của Bộ:

a) Tiểu ban Chỉ đạo An ninh mạng của Bộ đảm nhiệm chức năng Ban chỉ đạo ứng cứu khẩn cấp sự cố an ninh mạng của Bộ Nông nghiệp và Môi trường;

b) Cục Chuyển đổi số là Cơ quan thường trực Đội ứng cứu sự cố an ninh mạng của Bộ; rà soát trình Bộ kiện toàn Đội ứng cứu sự cố an ninh mạng của Bộ và tổ chức ứng cứu sự cố trong phạm vi của Bộ quản lý. Các đơn vị trực thuộc Bộ rà soát, cử cán bộ chuyên trách tham gia Đội ứng cứu sự cố an ninh mạng của Bộ theo đề nghị của Cục Chuyển đổi số.

2. Kế hoạch ứng phó sự cố an ninh mạng của Bộ:

a) Các đơn vị trực thuộc Bộ tổ chức xây dựng, phê duyệt kế hoạch ứng phó sự cố cho các hệ thống thông tin do đơn vị trực tiếp quản lý theo đề cương tại Phụ lục II của Quyết định số 05/2017/QĐ-TTg và tổ chức triển khai kế hoạch sau khi phê duyệt. Đối với các nội dung trong kế hoạch vượt thẩm quyền quyết định của đơn vị, đơn vị lấy ý kiến của Cục Chuyển đổi số, Vụ Kế hoạch - Tài chính (đối với các nội dung yêu cầu có kinh phí), báo cáo Bộ xem xét, quyết định;

b) Các kế hoạch ứng phó sự cố sau khi được phê duyệt phải gửi Cục Chuyển đổi số tổng hợp thành kế hoạch chung của Bộ. Cục Chuyển đổi số có trách nhiệm xây dựng kế hoạch ứng phó sự cố của Bộ, trình Lãnh đạo Bộ phê duyệt;

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

3. Quy trình ứng cứu sự cố an ninh mạng của Bộ:

a) Khi phát hiện dấu hiệu tấn công hoặc sự cố an ninh mạng, các cơ quan, đơn vị, tổ chức và cá nhân có trách nhiệm thông báo kịp thời cho đơn vị vận hành, đơn vị chủ quản hệ thống thông tin và Cục Chuyển đổi số. Cục Chuyển đổi số chịu trách nhiệm thiết lập, cập nhật thường xuyên và công khai danh sách đầu mối liên lạc, đường dây nóng sự cố của Bộ và các đơn vị trực thuộc trên Cổng thông tin điện tử của Bộ;

b) Khi xảy ra sự cố an ninh mạng thuộc loại hình tấn công mạng, đơn vị vận hành hệ thống thông tin thực hiện báo cáo theo quy định, đồng thời báo cáo Cục Chuyển đổi số để tổng hợp, báo cáo Tiểu ban Chỉ đạo An ninh mạng của Bộ.

c) Đường dây nóng:

- Tiếp nhận hỗ trợ và xử lý sự cố về an ninh mạng:

Trung tâm Hạ tầng số - Cục Chuyển đổi số: số điện thoại: 024.37956868 (Máy lẻ: 1005); email: hatangso@mae.gov.vn.

- Tiếp nhận báo cáo sự cố về an ninh mạng:

attt@mae.gov.vnPhòng An toàn thông tin - Cục Chuyển đổi số: email: attt@mae.gov.vn.

4. Diễn tập ứng cứu sự cố an ninh mạng của Bộ:

a) Chủ quản hệ thống thông tin tổ chức diễn tập ứng cứu sự cố theo kế hoạch ứng phó sự cố được phê duyệt;

b) Cục Chuyển đổi số chủ trì, phối hợp với các đơn vị thuộc Bộ tổ chức diễn tập ứng cứu sự cố trong phạm vi Bộ theo tần suất quy định tại điểm b Nhiệm vụ 4 mục II Điều 1 Quyết định số 1622/QĐ-TTg của Thủ tướng Chính phủ.

Điều 19. Đào tạo, bồi dưỡng nghiệp vụ, tuyên truyền, phổ biến nâng cao nhận thức về an ninh mạng

1. Các đơn vị trực thuộc Bộ xác định nhu cầu về đào tạo nguồn nhân lực bảo đảm an ninh mạng tại đơn vị mình, trình Bộ phê duyệt kế hoạch dài hạn, kế hoạch hàng năm về đào tạo, bồi dưỡng nghiệp vụ an toàn, an ninh thông tin cho công chức, viên chức và người lao động của Bộ.

2. Các đơn vị thuộc Bộ tổ chức đào tạo, bồi dưỡng nghiệp vụ về an ninh mạng cho cán bộ được giao thực hiện nhiệm vụ an ninh mạng; đào tạo cơ bản về an ninh mạng cho cán bộ quản lý, người sử dụng máy tính thuộc đơn vị theo kế hoạch hàng năm đã được phê duyệt.

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

4. Cục Chuyển đổi số xây dựng trình Bộ kế hoạch tuyên truyền, phổ biến nâng cao nhận thức về an ninh mạng tại Bộ và thực hiện các nội dung theo kế hoạch đã được phê duyệt.

Điều 20. Chế độ báo cáo an ninh mạng

1. Các loại báo cáo về an ninh mạng gồm:

a) Báo cáo công tác khắc phục mã độc, lỗ hổng, điểm yếu và triển khai cảnh báo an ninh mạng;

b) Báo cáo hoạt động giám sát của chủ quản hệ thống thông tin;

c) Báo cáo đột xuất theo yêu cầu của đơn vị chuyên trách về an ninh mạng của Bộ, Lãnh đạo Bộ hoặc cơ quan chức năng.

2. Trách nhiệm lập, phê duyệt báo cáo

a) Các đơn vị thuộc Bộ chịu trách nhiệm:

- Lập báo cáo an ninh mạng theo quy định tại điểm a khoản 1 Điều này, gửi Cục Chuyển đổi số trước ngày 20 tháng 11 hàng năm;

- Lập báo cáo hoạt động giám sát của chủ quản hệ thống thông tin theo quy định tại điểm b khoản 1 Điều này, gửi Cục Chuyển đổi số trước ngày 20 tháng 6 và 20 tháng 12 hàng năm;

- Báo cáo đột xuất theo quy định tại điểm c khoản 1 Điều này.

b) Cục Chuyển đổi số chịu trách nhiệm tập hợp, tổng hợp báo cáo của các đơn vị, trình Bộ phê duyệt, gửi các cơ quan quản lý nhà nước về an ninh mạng.

Chương III
QUY ĐỊNH VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN

Điều 21. Nguyên tắc bảo vệ dữ liệu cá nhân

1. Việc xử lý dữ liệu cá nhân tại các đơn vị thuộc Bộ phải đúng mục đích, trong phạm vi cần thiết, có căn cứ pháp lý, bảo đảm tính chính xác, an toàn, thời hạn lưu trữ và quyền của chủ thể dữ liệu cá nhân theo quy định pháp luật về bảo vệ dữ liệu cá nhân; quy định của pháp luật chuyên ngành và các quy định tại Quy chế này.

2. Phân cấp trách nhiệm bảo vệ dữ liệu cá nhân phù hợp với tổ chức bộ máy và quy chế làm việc của Bộ. Cơ quan, đơn vị thuộc Bộ phải xác định rõ trách nhiệm bảo vệ dữ liệu cá nhân, bố trí nhân sự hoặc bộ phận bảo vệ dữ liệu cá nhân theo quy định của Luật và Nghị định 356/2025/NĐ-CP.

3. Mỗi công chức, viên chức và người lao động tại các đơn vị thuộc Bộ nêu cao tinh thần chủ động, tự giác trong việc áp dụng các biện pháp bảo vệ dữ liệu cá nhân, góp phần ngăn chặn, xử lý hành vi vi phạm liên quan đến dữ liệu cá nhân theo quy định

của pháp luật; được đào tạo, hướng dẫn và chịu trách nhiệm trong phạm vi nhiệm vụ được giao.

Điều 22. Phân loại dữ liệu cá nhân được xử lý

1. Dữ liệu cá nhân được xử lý tại Bộ Nông nghiệp và Môi trường bao gồm:

a) Dữ liệu cá nhân phát sinh trong quá trình thực hiện chức năng, nhiệm vụ quản lý nhà nước của Bộ và của pháp luật khác có quy định cụ thể về trách nhiệm, nhiệm vụ của Bộ Nông nghiệp và Môi trường;

b) Dữ liệu cá nhân của công chức, viên chức và người lao động làm việc tại Bộ theo quy định của pháp luật về công chức, viên chức, thi đua, khen thưởng và pháp luật khác có liên quan;

c) Thông tin về tài khoản số của cá nhân và dữ liệu cá nhân phản ánh hoạt động, lịch sử hoạt động trên các hệ thống thông tin do Bộ Nông nghiệp và Môi trường, các đơn vị thuộc Bộ làm chủ quản theo quy định của pháp luật;

d) Dữ liệu cá nhân khác phát sinh trong hoạt động quản lý, thực hiện nhiệm vụ của các đơn vị thuộc Bộ không thuộc quy định tại điểm a, b và c khoản này.

2. Các trường hợp xử lý dữ liệu cá nhân mà không cần sự đồng ý của chủ thể dữ liệu:

a) Xử lý dữ liệu cá nhân thuộc điểm a, b và c khoản 1 Điều này khi đáp ứng điều kiện quy định tại Điều 19 Luật Bảo vệ dữ liệu cá nhân và quy định pháp luật có liên quan.

b) Xử lý dữ liệu cá nhân thu được từ hoạt động ghi âm, ghi hình tại trụ sở, nơi công cộng, hoạt động công cộng thuộc trường hợp quy định tại Điều 32 Luật Bảo vệ dữ liệu cá nhân. Đơn vị vận hành hệ thống camera phải thực hiện thông báo bằng biển báo hoặc hình thức phù hợp để chủ thể dữ liệu biết về hoạt động ghi âm, ghi hình, trừ trường hợp pháp luật có quy định khác.

c) Trường hợp thực hiện xử lý dữ liệu cá nhân không cần sự đồng ý của chủ thể dữ liệu phải thiết lập và duy trì cơ chế giám sát theo khoản 2 Điều 19 Luật Bảo vệ dữ liệu cá nhân, bao gồm quy trình và trách nhiệm xử lý, biện pháp bảo vệ phù hợp, đánh giá rủi ro và kiểm tra, đánh giá định kỳ việc tuân thủ, cơ chế tiếp nhận và xử lý phản ánh, kiến nghị.

3. Trường hợp xử lý dữ liệu cá nhân ngoài khoản 2 Điều này phải được sự đồng ý của chủ thể dữ liệu theo quy định tại Điều 9 Luật Bảo vệ dữ liệu cá nhân hoặc căn cứ xử lý khác theo quy định của Luật và pháp luật có liên quan.

4. Các đơn vị thuộc Bộ có hoạt động lưu trữ, xử lý dữ liệu cá nhân có trách nhiệm rà soát, phân loại, lập danh mục dữ liệu cá nhân đang xử lý (bao gồm dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm). Việc xử lý dữ liệu cá nhân nhạy cảm phải được thiết lập quy trình bảo vệ độc lập, phân quyền truy cập, khai thác nghiêm ngặt và tuân thủ các điều kiện chặt chẽ theo quy định của Luật Bảo vệ dữ liệu cá nhân, Nghị định số 356/2025/NĐ-CP ngày 31 tháng 12 năm 2025 của Chính phủ quy định chi tiết

một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân và các quy định pháp luật khác có liên quan.

Điều 23. Xác định các vai trò theo quy định của pháp luật về bảo vệ dữ liệu cá nhân

1. Việc xác định "Bên kiểm soát dữ liệu cá nhân", "Bên kiểm soát và xử lý dữ liệu cá nhân", "Bên xử lý dữ liệu cá nhân" và các bên có liên quan được thực hiện căn cứ vào mục đích, phương tiện, phạm vi và thực tế tham gia hoạt động xử lý dữ liệu cá nhân theo quy định của Luật Bảo vệ dữ liệu cá nhân.

2. Đơn vị có hoạt động xử lý dữ liệu cá nhân chủ động xác định các vai trò "Bên Kiểm soát dữ liệu cá nhân", "Bên Kiểm soát và xử lý dữ liệu cá nhân", "Bên xử lý dữ liệu cá nhân" (nếu có), đồng thời phải được thể hiện bằng hồ sơ, văn bản phân công, thỏa thuận chia sẻ dữ liệu hoặc hợp đồng xử lý dữ liệu đối với dữ liệu cá nhân được thu thập, lưu trữ, xử lý thuộc phạm vi chức năng, nhiệm vụ được giao theo quy định tại khoản 1 Điều 22 của Quy chế này.

Điều 24. Bảo vệ dữ liệu cá nhân trong quá trình xử lý dữ liệu cá nhân bên ngoài hệ thống thông tin xử lý dữ liệu cá nhân

1. Dữ liệu cá nhân phải được xử lý trong phạm vi quy định của pháp luật. Cá nhân, đơn vị thực hiện xử lý dữ liệu cá nhân có trách nhiệm:

a) Trước khi thu thập, lưu trữ, xử lý dữ liệu cá nhân, phải xác định rõ căn cứ pháp lý cho việc xử lý dữ liệu cá nhân (Điều, khoản của văn bản quy phạm pháp luật quy định mục đích và phạm vi dữ liệu cá nhân được phép xử lý).

b) Trường hợp được yêu cầu tiếp nhận, xử lý dữ liệu cá nhân ngoài phạm vi chức năng, nhiệm vụ hoặc ngoài căn cứ pháp lý được xác định, đơn vị không được thực hiện khi chưa xác định được căn cứ pháp lý và thẩm quyền xử lý. Trường hợp pháp luật cho phép xử lý trên cơ sở sự đồng ý thì phải thực hiện việc xin sự đồng ý theo quy định của Luật Bảo vệ dữ liệu cá nhân.

c) Không sử dụng tài khoản cá nhân, mạng xã hội, ứng dụng nhắn tin công cộng hoặc phương tiện không được cơ quan có thẩm quyền cho phép để trao đổi, truyền đưa dữ liệu cá nhân trong hoạt động công vụ.

2. Công chức, viên chức và người lao động được phân công xử lý dữ liệu cá nhân có trách nhiệm:

a) Không cung cấp, chia sẻ dữ liệu cá nhân đã thu thập cho tổ chức, cá nhân không thuộc phạm vi phải cung cấp theo quy định của pháp luật.

b) Sử dụng máy tính đáp ứng yêu cầu về an toàn an ninh mạng: cài đặt phần mềm phòng, diệt mã độc; xử lý lỗ hổng bảo mật (nếu có) và được kiểm tra an ninh mạng.

c) Áp dụng mã hóa tệp dữ liệu khi thực hiện trao đổi dữ liệu cá nhân trên môi trường mạng hoặc mang dữ liệu cá nhân ra khỏi cơ quan bằng thiết bị, phương tiện điện tử (trừ dữ liệu thuộc danh mục bí mật nhà nước thực hiện theo quy định của pháp luật về bảo vệ bí mật nhà nước). Không sử dụng mạng xã hội, tài khoản cá nhân, ứng

dụng nhắn tin công cộng hoặc phương tiện không được cơ quan có thẩm quyền cho phép để trao đổi, truyền đưa dữ liệu cá nhân trong hoạt động công vụ.

d) Kiểm soát chặt các phiên bản bản điện tử, bản in chứa dữ liệu cá nhân; giới hạn truy cập tới dữ liệu cá nhân trong phạm vi các cá nhân có trách nhiệm tham gia kiểm soát và xử lý dữ liệu cá nhân; xóa, hủy dữ liệu cá nhân đã được lưu giữ khi đã hoàn thành mục đích sử dụng hoặc hết thời hạn lưu trữ; xóa không thể khôi phục được hoặc hủy các thiết bị chứa dữ liệu cá nhân khi không còn tiếp tục sử dụng.

Điều 25. Bảo vệ dữ liệu cá nhân trong quá trình xử lý dữ liệu cá nhân trên hệ thống thông tin xử lý dữ liệu cá nhân

1. Đơn vị tham gia sử dụng hệ thống thông tin xử lý dữ liệu cá nhân có trách nhiệm xác định chính xác các cá nhân được phép truy cập hệ thống thông tin để xử lý dữ liệu cá nhân theo hướng đúng người, đúng nhiệm vụ, đúng phạm vi, đúng thời hạn và bảo đảm nguyên tắc phân quyền tối thiểu; gửi đề nghị thay đổi, thu hồi tài khoản truy cập hệ thống thông tin tới đơn vị vận hành hệ thống thông tin ngay sau khi có sự thay đổi phân công về xử lý dữ liệu cá nhân tại đơn vị.

2. Cá nhân được cấp tài khoản truy cập hệ thống thông tin để xử lý dữ liệu cá nhân trên hệ thống có trách nhiệm:

a) Bảo mật thông tin xác thực của tài khoản được cấp; không cung cấp thông tin xác thực cho người không có thẩm quyền hoặc không được giao nhiệm vụ đối với hệ thống thông tin.

b) Không thực hiện các hoạt động xử lý hoặc khai thác dữ liệu cá nhân trên hệ thống thông tin ngoài phạm vi trách nhiệm, nhiệm vụ được phân công.

c) Chỉ xử lý dữ liệu cá nhân trên các trang thiết bị, máy tính trong hệ thống thông tin xử lý dữ liệu cá nhân được bảo đảm an toàn, an ninh mạng theo quy định pháp luật.

d) Khi không còn được phân công xử lý dữ liệu cá nhân trên hệ thống thông tin, phải yêu cầu đơn vị quản lý thực hiện thay đổi, thu hồi tài khoản; có trách nhiệm bàn giao công việc, dữ liệu và tài liệu liên quan cho người tiếp nhận theo phân công của đơn vị quản lý; không bàn giao thông tin xác thực tài khoản.

Điều 26. Bảo đảm an ninh mạng hệ thống thông tin xử lý dữ liệu cá nhân

1. Đối với các hệ thống thông tin xử lý dữ liệu cá nhân (được xây dựng, nâng cấp sau thời điểm Quy chế này có hiệu lực), phải nêu rõ căn cứ pháp luật của việc xử lý thông tin tại thuyết minh chủ trương đầu tư, dự án, kế hoạch thuê dịch vụ.

2. Bảo đảm an ninh mạng theo Điều 7 của Quy chế này.

3. Hệ thống thông tin thu thập, lưu trữ, xử lý dữ liệu cá nhân phải có tính năng ghi và lưu trữ nhật ký hệ thống quá trình xử lý dữ liệu cá nhân; hệ thống phải hỗ trợ cung cấp thông tin trên giao diện người dùng về mục đích, phạm vi và căn cứ xử lý dữ liệu cá nhân theo quy định của pháp luật và chính sách bảo vệ dữ liệu cá nhân của đơn vị.

4. Áp dụng các biện pháp xác thực, phân quyền truy cập, mã hóa dữ liệu và mã hóa kênh kết nối truyền nhận dữ liệu cá nhân giữa các hệ thống thông tin, giữa người

dùng và hệ thống thông tin phù hợp với tính chất, mức độ nhạy cảm và rủi ro của dữ liệu.

5. Không xử lý dữ liệu cá nhân trên hệ thống thông tin thử nghiệm (sử dụng thông tin giả lập, mô phỏng dữ liệu cá nhân trên hệ thống thông tin thử nghiệm nếu cần thiết), trừ trường hợp được cho phép theo quy định. Trường hợp cần thử nghiệm, chỉ được phép sử dụng dữ liệu không phải dữ liệu cá nhân, dữ liệu cá nhân đã được khử nhận dạng hoặc áp dụng kỹ thuật ẩn danh dữ liệu cá nhân tuân theo quy chuẩn và quy định của pháp luật.

6. Kiểm tra, đánh giá tuân thủ quy định của pháp luật về bảo vệ dữ liệu cá nhân đồng thời với việc kiểm tra, đánh giá an toàn, an ninh mạng đối với hệ thống thông tin.

7. Thực hiện xóa, hủy toàn bộ dữ liệu cá nhân trên hệ thống thông tin thu thập, lưu trữ, xử lý dữ liệu cá nhân khi hệ thống kết thúc vận hành, trừ trường hợp được phép lưu trữ theo quy định pháp luật.

Điều 27. Bảo vệ dữ liệu cá nhân trong hoạt động biên tập, công khai thông tin trên trang/cổng thông tin điện tử, dịch vụ công trực tuyến

Đơn vị vận hành trang/cổng thông tin điện tử, dịch vụ công trực tuyến có trách nhiệm triển khai các biện pháp kiểm soát, ngăn ngừa việc hiển thị hoặc công khai dữ liệu cá nhân không đúng quy định trên trang/Cổng Thông tin điện tử, dịch vụ công trực tuyến; không để lộ lọt, công khai dữ liệu cá nhân không đúng quy định của pháp luật từ trang/cổng thông tin điện tử, dịch vụ công trực tuyến và hoạt động biên tập trang/cổng thông tin điện tử:

1. Bổ sung vào quy trình biên tập tin, bài viết yêu cầu phải rà soát dữ liệu cá nhân trong nội dung bài viết trước khi đăng trên cổng, trang thông tin điện tử. Chỉ được công khai dữ liệu cá nhân khi có căn cứ pháp lý, đúng mục đích, phạm vi và điều kiện công khai theo quy định của pháp luật. Không đăng công khai dữ liệu cá nhân nhạy cảm trên cổng, trang thông tin điện tử, dịch vụ công trực tuyến, trừ trường hợp pháp luật quy định.

2. Rà soát, bảo đảm các trường thông tin được hiển thị trên trang/cổng thông tin, dịch vụ công trực tuyến không vi phạm quy định của pháp luật về bảo vệ dữ liệu cá nhân, kịp thời gỡ bỏ thông tin không cần thiết hoặc có nguy cơ gây lộ dữ liệu cá nhân.

3. Khuyến khích hiển thị cảnh báo về rủi ro lộ, lọt dữ liệu cá nhân đối với các chuyên mục có khả năng công khai thông tin do người dùng nhập (trường hợp câu hỏi của người dùng chứa dữ liệu cá nhân); áp dụng công cụ kỹ thuật để kiểm soát nội dung chứa dữ liệu cá nhân hiển thị trên trang/cổng thông tin điện tử, dịch vụ công trực tuyến.

Điều 28. Đánh giá tác động xử lý dữ liệu cá nhân

1. Trường hợp "Bên Kiểm soát dữ liệu cá nhân", "Bên Kiểm soát và xử lý dữ liệu cá nhân" là Bộ Nông nghiệp và Môi trường, Cục Chuyển đổi số có trách nhiệm:

a) Phối hợp các đơn vị liên quan xây dựng, gửi Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân, Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài (nếu có) cho Bộ Công an theo hướng dẫn tại Nghị định số 356/2025/NĐ-CP.

b) Lưu giữ 01 bản hồ sơ, sẵn sàng phục vụ hoạt động kiểm tra, đánh giá của Bộ Công an;

c) Phối hợp với các đơn vị liên quan cập nhật, hoàn thiện hồ sơ khi có sự thay đổi về nội dung hồ sơ đã gửi Bộ Công an theo quy định.

2. Trường hợp Bên Kiểm soát dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân là đơn vị thuộc Bộ, các đơn vị có trách nhiệm:

a) Tổ chức xây dựng, ban hành quyết định phê duyệt Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân, Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân ra nước ngoài (nếu có);

b) Gửi hồ sơ cho Bộ Công an theo hướng dẫn tại Nghị định số 356/2025/NĐ-CP, đồng thời gửi bản điện tử của hồ sơ cho Cục Chuyển đổi số để phục vụ công tác quản lý về bảo vệ dữ liệu cá nhân của Bộ;

c) Lưu giữ 01 bản hồ sơ, sẵn sàng phục vụ hoạt động kiểm tra, đánh giá của Bộ Công an và của Bộ;

d) Cập nhật Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân và Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới theo Điều 20 Nghị định số 356/2025/NĐ-CP.

3. Đơn vị thuộc Bộ khi thuê bên xử lý dữ liệu cá nhân phải quy định trong hợp đồng/thỏa thuận về trách nhiệm của bên xử lý trong việc lập, lưu giữ, cung cấp hồ sơ đánh giá tác động và tài liệu chứng minh việc tuân thủ pháp luật về bảo vệ dữ liệu cá nhân khi được yêu cầu theo quy định của pháp luật và Quy chế này.

4. Đơn vị thuộc Bộ trước khi thực hiện hoạt động có khả năng làm phát sinh chuyển dữ liệu cá nhân xuyên biên giới phải xác định việc chuyển dữ liệu thuộc trường hợp quy định tại Điều 20 Luật Bảo vệ dữ liệu cá nhân và Điều 17 Nghị định số 356/2025/NĐ-CP; trường hợp thuộc diện phải lập hồ sơ đánh giá tác động thì phải hoàn thành các yêu cầu theo quy định trước khi thực hiện chuyển dữ liệu, trừ trường hợp pháp luật có quy định khác.

5. Việc lập, cập nhật, lưu giữ, gửi Bộ Công an Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân và Hồ sơ đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới được thực hiện theo các Điều 18, Điều 19 và Điều 20 Nghị định số 356/2025/NĐ-CP và các văn bản sửa đổi, bổ sung, thay thế (nếu có).

Điều 29. Thông báo và xử lý trường hợp vi phạm quy định của pháp luật về bảo vệ dữ liệu cá nhân

1. Khi phát hiện hành vi vi phạm quy định của pháp luật về bảo vệ dữ liệu cá nhân, đơn vị, cá nhân phát hiện phải kịp thời ghi nhận, bảo vệ dữ liệu và thông tin liên quan, áp dụng biện pháp ngăn chặn, hạn chế tác hại và thông báo cho đầu mối có trách nhiệm về bảo vệ dữ liệu cá nhân của đơn vị.

2. Trường hợp vi phạm thuộc trường hợp phải thông báo theo Điều 23 Luật Bảo vệ dữ liệu cá nhân, Bên kiểm soát dữ liệu cá nhân, Bên kiểm soát và xử lý dữ liệu cá nhân, Bên thứ ba có trách nhiệm thông báo cho cơ quan chuyên trách bảo vệ dữ liệu

cá nhân chậm nhất 72 giờ kể từ khi phát hiện hành vi vi phạm. Nội dung và phương thức thông báo thực hiện theo Điều 28 Nghị định số 356/2025/NĐ-CP.

3. Trường hợp công chức, viên chức và người lao động (sau đây gọi chung là cá nhân) làm việc tại các đơn vị thuộc Bộ có hành vi vi phạm quy định về bảo vệ dữ liệu cá nhân:

a) Nếu cá nhân thuộc thẩm quyền quản lý của Bộ trưởng, đơn vị trực tiếp quản lý cá nhân có hành vi vi phạm phối hợp với Cục Chuyển đổi số đánh giá, xác định mức độ vi phạm và báo cáo Bộ xem xét, xử lý.

b) Nếu cá nhân thuộc thẩm quyền quản lý của thủ trưởng các đơn vị thuộc Bộ, đơn vị trực tiếp quản lý cá nhân có hành vi vi phạm báo cáo thủ trưởng các đơn vị thuộc Bộ xem xét, xử lý.

c) Đối với các trường hợp không thuộc phạm vi quy định tại điểm a, b khoản này, thủ trưởng đơn vị trực tiếp quản lý cá nhân có trách nhiệm xác định mức độ vi phạm và quyết định biện pháp xử lý phù hợp với quy định của pháp luật.

d) Trường hợp vi phạm quy định của pháp luật về bảo vệ dữ liệu cá nhân, cấp có thẩm quyền quyết định về công tác nhân sự đối với cá nhân vi phạm (theo quy định về phân cấp quản lý công chức, viên chức tại các đơn vị thuộc và trực thuộc Bộ) và thông báo đến cơ quan chuyên trách bảo vệ dữ liệu cá nhân theo quy định pháp luật về bảo vệ dữ liệu cá nhân.

4. Trường hợp hành vi vi phạm quy định của pháp luật về bảo vệ dữ liệu cá nhân thuộc lĩnh vực quản lý nhà nước của Bộ do các đối tượng không thuộc phạm vi quản lý của Bộ thực hiện, Bên kiểm soát dữ liệu cá nhân, Bên kiểm soát và xử lý dữ liệu cá nhân, Bên xử lý dữ liệu cá nhân, Bên thứ ba (nếu có) gửi thông báo vi phạm quy định về dữ liệu cá nhân đến cơ quan chuyên trách bảo vệ dữ liệu cá nhân thuộc Bộ Công an để xử lý theo quy định pháp luật về bảo vệ dữ liệu cá nhân.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 30. Kinh phí thực hiện

1. Kinh phí bảo đảm an ninh mạng được bố trí trong dự toán chi thường xuyên hằng năm hoặc được lồng ghép, tích hợp trong các chương trình, dự án, nhiệm vụ sử dụng ngân sách nhà nước và từ các nguồn kinh phí hợp pháp khác. Đối với nhiệm vụ, dự án có nội dung đầu tư, xây dựng, thiết lập, nâng cấp hoặc mở rộng hệ thống thông tin, kinh phí bảo đảm an ninh mạng phải được xác định, bố trí ngay trong tổng mức đầu tư hoặc dự toán của nhiệm vụ, dự án, bảo đảm tỷ lệ tối thiểu theo quy định của pháp luật về an ninh mạng.

2. Căn cứ kế hoạch hằng năm và yêu cầu bảo vệ hệ thống thông tin theo cấp độ, các đơn vị thuộc Bộ có trách nhiệm lập dự toán kinh phí cho hoạt động bảo đảm an ninh mạng, gửi Vụ Kế hoạch - Tài chính thẩm định, trình cấp có thẩm quyền phê duyệt theo quy định. Việc quản lý, sử dụng và quyết toán kinh phí thực hiện theo

quy định của pháp luật về ngân sách nhà nước, đầu tư công và các quy định pháp luật có liên quan.

Điều 31. Trách nhiệm của Cục Chuyển đổi số

1. Thực hiện các trách nhiệm được giao tại Quy chế này.

2. Hướng dẫn triển khai Quy chế này và các quy định liên quan của Chính phủ, Nhà nước về an ninh mạng.

3. Tổ chức triển khai thực hiện Quy chế tại khối cơ quan Bộ.

4. Xây dựng kế hoạch, báo cáo về an ninh mạng của Bộ Nông nghiệp và Môi trường.

5. Thẩm định, cho ý kiến chuyên môn về nội dung, dự toán kinh phí các dự án, nhiệm vụ có liên quan đến an ninh mạng theo quy định.

6. Bảo đảm an ninh mạng cho hệ thống mạng nội bộ, các hệ thống thông tin, cơ sở dữ liệu dùng chung của Bộ, các hệ thống thông tin do Văn phòng Bộ, các Vụ thuộc Bộ quản lý, sử dụng và các hệ thống thông tin khác theo quyết định của Bộ trưởng.

Điều 32. Trách nhiệm của các đơn vị thuộc Bộ

1. Thực hiện các trách nhiệm được giao tại Quy chế này.

2. Tổ chức triển khai thực hiện Quy chế này tại đơn vị.

3. Thực hiện các báo cáo theo quy định, gửi Cục Chuyển đổi số tổng hợp, báo cáo Bộ.

4. Xây dựng, triển khai Quy chế bảo đảm an ninh mạng tại đơn vị bảo đảm phù hợp với Quy chế này và các yêu cầu cụ thể của đơn vị.

5. Vận hành hệ thống mạng nội bộ, các hệ thống thông tin, cơ sở dữ liệu theo khoản 2 Điều 5 của Quy chế này.

6. Đối với Văn phòng Bộ, các Vụ: Phối hợp với Cục Chuyển đổi số bảo đảm an ninh mạng cho các hệ thống thông tin, cơ sở dữ liệu dùng chung của Bộ và các hệ thống thông tin do đơn vị quản lý, vận hành.

Điều 33. Trách nhiệm của chủ quản hệ thống thông tin

1. Thực hiện trách nhiệm của đơn vị chủ quản hệ thống thông tin theo quy định tại Quy chế này.

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

3. Chỉ đạo rà soát, xác định các hệ thống thông tin quan trọng về an ninh quốc gia theo Điều 16 Nghị định số 331/2026/NĐ-CP.

Điều 34. 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 Quy chế này và các nhiệm vụ do chủ quản hệ thống thông tin phân công.

2. Chỉ đạo, phân công các bộ phận kỹ thuật thuộc đơn vị (quản lý mạng; quản lý ứng dụng; quản lý dữ liệu; vận hành hệ thống thông tin; triển khai và hỗ trợ kỹ thuật) triển khai công tác bảo đảm an ninh mạng trong tất cả các công đoạn liên quan đến hệ thống thông tin.

Điều 35. 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: 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 Bộ về các vi phạm, thất thoát thông tin, dữ liệu thuộc phạm vi quản lý của đơn vị do không tổ chức, chỉ đạo, kiểm tra cán bộ của đơn vị thực hiện đúng quy định.

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

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

Điều 36. Khen thưởng, kỷ luật

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

2. Đơn vị, cá nhân vi phạm Quy chế này và các quy định khác của pháp luật về an ninh 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 37. Trách nhiệm thi hành

1. Thủ trưởng các đơn vị trực thuộc Bộ có trách nhiệm phổ biến, quán triệt đến toàn bộ công chức, viên chức và 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 Cục Chuyển đổi số để tổng hợp, trình Bộ trưởng xem xét, sửa đổi, bổ sung Quy chế./.