BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 1921/QĐ-BNNMT	*Hà Nội, ngày 05 tháng 6 năm 2025*

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Bộ Nông nghiệp và Môi trường

BỘ TRƯỞNG BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG

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 Nghị định số 147/2024/NĐ-CP ngày 09 tháng 11 năm 2024 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng;

Căn cứ Nghị định số 35/2025/NĐ-CP ngày 25 tháng 02 năm 2025 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 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 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 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 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 Tiêu chuẩn Việt Nam TCVN 11930:2017 Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ;

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 toàn thông tin mạng, an ninh mạng Bộ Nông nghiệp và Môi trường.

Điều 2. Quyết định này có hiệu lực từ ngày ký và thay thế các Quyết định: Quyết định số 2390/QĐ-BTNMT ngày 18 tháng 8 năm 2023 của Bộ trưởng Bộ Tài nguyên và Môi trường Ban hành Quy chế bảo đảm an toàn, an ninh thông tin mạng Bộ Tài nguyên và Môi trường; Quyết định số 3747/QĐ-BNN-KHCN ngày 05 tháng 9 năm 2023 của Bộ trưởng Bộ Nông nghiệp và Phát triển nông thôn Ban hành Quy chế an toàn thông tin mạng và an ninh mạng Bộ Nông nghiệp và Phát triển nông thôn.

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, các Thứ trưởng;
- Sở NN và MT các tỉnh, TP trực thuộc trung ương;
- Cổng thông tin điện tử Bộ;
- Lưu: VT, CĐS.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG

Trần Quý Kiên

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 TOÀN THÔNG TIN MẠNG, AN NINH MẠNG BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG

(Kèm theo Quyết định số /QĐ-BNNMT ngày tháng năm 2025 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 toàn thông tin mạng, 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 và an toàn thông tin mạng, 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 toàn thông tin mạng* là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

2. *An ninh mạng* là việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

3. *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.

4. *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…

5. *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.

6. *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.

7. *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.

8. *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.

9. *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.

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. *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.

13. *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, an ninh thông tin mạng

1. Bảo đảm an toàn, an ninh thông tin 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 toàn, an ninh thông tin tuân thủ các nguyên tắc chung quy định tại Điều 4 Luật An toàn thông tin mạng và Điều 4 Nghị định số 85/2016/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 toàn, an ninh thông tin 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 toàn thông tin mạng và 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 toàn 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 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 73/2019/NĐ-CP và khoản 1, Điều 1 của Nghị định số 82/2024/NĐ-CP phải có ý kiến thẩm định nội dung liên quan đến an toàn, an ninh thông tin, 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 khác phải bảo đảm quy định của pháp luật về bảo vệ bí mật nhà nước.

6. Xử lý sự cố an toàn thông tin 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 toàn thông tin 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 toàn, an ninh mạng.

Điều 4. Các hành vi bị nghiêm cấm

1. Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật An toàn thông tin mạng, Điều 8 Luật An ninh mạng và Điều 5 Luật Bảo vệ bí mật nhà nước.

2. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập mạng không dây của cá nhân vào mạng nội bộ; tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin cài đặt trên thiết bị công nghệ thông tin phục vụ công việc; tự ý thay thế, lắp mới, tráo đổi thành phần của máy tính phục vụ công việc.

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

4. Sử dụng hạ tầng, trang thiết bị công nghệ thông tin của cơ quan, đơn vị để đào tiền ảo, đánh bạc, cá độ.

5. Phát tán thư rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.

6. Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân.

7. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

8. Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới khả năng truy cập hệ thống thông tin của người sử dụng.

9. Các hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

Chương II
QUY ĐỊNH BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG, AN NINH MẠNG

Điều 5. Phân công thực hiện các vai trò về bảo đảm an toàn thông tin 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 thông qua một trong các văn bản sau: Thông tư của Bộ Nông nghiệp và Môi trường hoặc Quyết định của Bộ trưởng Bộ Nông nghiệp và Môi trường có nội dung giao đơn vị làm nhiệm vụ quản lý hệ thống thông tin; quyết định phê duyệt dự án, trong đó giao đơn vị làm chủ đầu tư dự án; văn bản ủy quyền theo quy định tại khoản 3 Điều 4 Thông tư số 12/2022/TT-BTTTT;

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 Thông tư số 12/2022/TT-BTTTT và thực hiện trách nhiệm theo quy định tại Điều 20 Nghị định số 85/2016/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 Khoản 1, Khoản 2 Điều 5 Thông tư số 12/2022/TT-BTTTT;

d) Trường hợp thuê dịch vụ công nghệ thông tin, đơn vị vận hành được xác định theo Khoản 3 Điều 5 Thông tư số 12/2022/TT-BTTTT.

3. Đơn vị chuyên trách về an toàn thông tin

a) Cục Chuyển đổi số là đơn vị chuyên trách về an toàn thông tin của Bộ;

b) Đơn vị chuyên trách về công nghệ thông tin, chuyển đổi số tại các đơn vị trực thuộc Bộ đồng thời là đơn vị chuyên trách về an toàn thông tin.

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. Nội dung của hồ sơ đề xuất cấp độ hệ thống thông tin quy định tại Điều 15 Nghị định số 85/2016/NĐ-CP và Điều 8, Điều 9 Thông tư số 12/2022/TT-BTTTT.

3. Nội dung, thời gian thẩm định hồ sơ đề xuất cấp độ hệ thống thông tin quy định tại Điều 16 Nghị định số 85/2016/NĐ-CP.

4. Thẩm quyền, trình tự, thủ tục xác định cấp độ hệ thống thông tin quy định tại Điều 12, Điều 13, Điều 14 Nghị định số 85/2016/NĐ-CP và Điều 6 Thông tư số 12/2022/TT-BTTTT.

Điều 7. Phương án bảo đảm an toàn hệ thống thông tin

1. Phương án bảo đảm an toàn hệ thống thông tin đối với từng cấp độ phải đáp ứng yêu cầu quy định tại Điều 10 Thông tư số 12/2022/TT-BTTTT, phù hợp với tiêu chuẩn TCVN 11930:2017, các tiêu chuẩn, quy chuẩn kỹ thuật và chính sách an toàn thông tin mạng của Bộ, chính sách an toàn thông tin mạng của các đơn vị trực thuộc Bộ (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 toàn hệ thống thông tin sau khi hồ sơ đề xuất cấp độ hoặc phương án bảo đảm an toàn hệ thống được phê duyệt.

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

4. Đơn vị vận hành phải xây dựng Quy chế bảo đảm an toàn, an ninh mạng cho hệ thống thông tin đáp ứng các yêu cầu về quản lý theo cấp độ an toàn 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 toàn, an ninh thông tin 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 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 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 toàn, an ninh thông tin;

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 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 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 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 9. Quản lý an toàn, an ninh thông tin 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 toàn, an ninh thông tin 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 toàn thông tin riêng), bao gồm: vùng mạng người dùng; vùng mạng kết nối hệ thống ra bên ngoài Internet và các mạng khác; vùng mạng máy chủ công cộng; vùng mạng máy chủ nội bộ; vùng mạng máy chủ quản trị;

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

- 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 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;

- 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 toàn thông tin 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 mất an toàn thông tin.

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