BỘ NÔNG NGHIỆP VÀ PHÁT TRIỂN NÔNG THÔN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 3747 /QĐ-BNN-KHCN	*Hà Nội, ngày 05 tháng 9 năm 2023*

QUYẾT ĐỊNH
Ban hành Quy chế An toàn thông tin mạng và An ninh mạng Bộ Nông nghiệp và Phát triển nông thôn

BỘ TRƯỞNG BỘ NÔNG NGHIỆP VÀ PHÁT TRIỂN NÔNG THÔN

Căn cứ Nghị định số 105/2022/NĐ-CP ngày 22 tháng 12 năm 2022 của Chính phủ Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Nông nghiệp và Phát triển nông thôn;

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Luật An ninh mạng ngày 12 tháng 6 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 15/8/2022 của Chính phủ về việc quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Nghị định số 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 của Chính phủ về bảo vệ dữ liệu cá nhân;

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

Căn cứ Thông tư số 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 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;

Xét Công văn số 231/CĐS ngày 25 tháng 8 năm 2023 của Trung tâm Chuyển đổi số và Thống kê nông nghiệp về trình Bộ ban hành Quy chế ATTT mạng và An ninh mạng của Bộ và kèm theo Hồ sơ;

Theo đề nghị của Vụ trưởng Vụ Khoa học, Công nghệ và Môi trường.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Quy chế An toàn thông tin mạng và An ninh mạng Bộ Nông nghiệp và Phát triển nông thôn".

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

Điều 3. Chánh Văn phòng Bộ, Vụ trưởng Vụ Khoa học, Công nghệ và Môi trường, Giám đốc Trung tâm Chuyển đổi số và Thống kê nông nghiệp, Thủ trưởng các đơn vị thuộc Bộ; các cơ quan, đơn vị, tổ chức và cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ trưởng (để báo cáo);
- Các Thứ trưởng (để báo cáo);
- Ban chỉ đạo CĐS của Bộ;
- Đội ƯCSC ATTT mạng Bộ;
- Các đơn vị thuộc Bộ;
- Bộ Thông tin và Truyền thông;
- Cổng thông tin điện tử Bộ;
- Lưu: VT, KHCN (KTD.05).

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

BỘ NÔNG NGHIỆP VÀ PHÁT TRIỂN NÔNG THÔN

Nguyễn Hoàng Hiệp

BỘ NÔNG NGHIỆP VÀ PHÁT TRIỂN NÔNG THÔN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY CHẾ
An toàn thông tin mạng và An ninh mạng Bộ Nông nghiệp và PTNT

(Kèm theo Quyết định số /QĐ-BNN-KHCN ngày tháng năm 2023 của Bộ Nông nghiệp và Phát triển nông thôn)

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 ứng dụng công nghệ thông tin, phát triển chính phủ điện tử, chính phủ số, chuyển đổi số của Bộ Nông nghiệp và Phát triển nông thôn (sau đây gọi tắt là Bộ).

2. Đối tượng áp dụng:

a) Quy chế này áp dụng với các cơ quan, đơn vị hành chính, sự nghiệp thuộc cơ cấu tổ chức của Bộ theo Nghị định số 105/NĐ-CP ngày 22/12/2022 của Chính phủ Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Nông nghiệp và Phát triển nông thôn (sau đây gọi tắt là đơn vị).

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, chính phủ điện tử, chính phủ số 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 sự bảo đảm 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.

3. *Mạng* là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính.

4. *Hệ thống thông tin* là tập hợp phần cứng, phần mềm và 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. *Trang thiết bị công nghệ thông tin* là một nhóm hay một dòng sản phẩm cố định có khả năng xử lý dữ liệu và truyền tải thông tin dữ liệu qua lại giữa những người sử dụng.

7. *Thiết bị xử lý thông tin* là thiết bị dùng để tạo lập, xử lý, lưu trữ, truyền đưa thông tin dưới dạng điện tử (máy tính, máy in, điện thoại thông minh, thiết bị mạng, thiết bị an ninh mạng, camera giám sát và các thiết bị tương đương khác).

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

9. *Phần mềm độc hại* là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

10. *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 mạng

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

2. Phân cấp, ủy quyền trách nhiệm bảo đảm an toàn, an ninh mạng phù hợp với tổ chức bộ máy và phương thức làm việc của Bộ.

3. An toàn thông tin mạng phải gắn liền và hỗ trợ các hoạt động giao dịch điện tử, ứng dụng công nghệ thông tin, chính phủ điện tử, chính phủ số, chuyển đổi số của Bộ; hỗ trợ việc sử dụng trang thiết bị công nghệ thông tin, thiết bị xử lý thông tin để xử lý công việc của cán bộ, công chức, viên chức, người lao động của Bộ.

4. Ứng cứu sự cố an toàn thông tin mạng là hoạt động quan trọng nhằm phát hiện, ngăn chặn, xử lý và khắc phục kịp thời sự cố an toàn an ninh mạng.

5. 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.

6. Mỗi cán bộ, 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.

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

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

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

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

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

Chương II
QUY ĐỊNH BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN 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 Phát triển nông thôn 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 Phát triển nông thôn 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 Phát triển nông thôn hoặc

Quyết định của Bộ trưởng Bộ Nông nghiệp và Phát triển nông thôn 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 ngày 12/8/2022.

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) theo quy định tại Điều 4 Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 và thực hiện trách nhiệm theo quy định tại Điều 20 Nghị định 85/2016/NĐ-CP ngày 01/7/2016.

2. Đơn vị vận hành hệ thống thông tin:

a) Đơn vị thuộc Bộ chủ trì xây dựng, thiết lập, nâng cấp, mở rộng, bảo trì, bảo dưỡng, duy trì hoạt động lớp ứng dụng hoặc cơ sở dữ liệu của hệ thống thông tin thực hiện vai trò đơn vị vận hành hệ thống thông tin. Trung tâm Chuyển đổi số và Thống kê nông nghiệp là đơn vị vận hành hệ thống mạng nội bộ, hệ thống an toàn an ninh mạng, các hệ thống thông tin, cơ sở dữ liệu dùng chung của Bộ, các hệ thống thông tin do Thanh tra Bộ, các Vụ thuộc Bộ làm chủ quản (nếu có yêu cầu) và các hệ thống thông tin khác theo quyết định của Bộ trưởng.

b) Trường hợp hệ thống thông tin đang trong thời gian thuê dịch vụ công nghệ thông tin, đơn vị cung cấp dịch vụ thực hiện vai trò đơn vị vận hành hệ thống thông tin.

c) Các hệ thống thông tin trước khi đưa vào khai thác, sử dụng phải được giao cho đơn vị vận hành. Đơn vị vận hành hệ thống thông tin theo quy định tại Điều 5 Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 và thực hiện trách nhiệm theo quy định tại Điều 22 Nghị định 85/2016/NĐ-CP ngày 01/7/2016.

3. Đơn vị chuyên trách về an toàn thông tin:

a) Trung tâm Chuyển đổi số và Thống kê nông nghiệp đảm nhiệm vai trò đơn vị chuyên trách về an toàn thông tin mạng của Bộ Nông nghiệp và Phát triển nông thôn.

b) Chủ quản hệ thống thông tin thành lập hoặc chỉ định bộ phận chuyên trách an toàn thông tin mạng thuộc đơn vị chuyên trách an toàn thông tin mạng của chủ quản hệ thống thông tin.

c) Đơn vị chuyên trách về an toàn thông tin thực hiện trách nhiệm theo quy định tại Điều 21 Nghị định 85/2016/NĐ-CP ngày 01/7/2016.

Điều 6. Thẩm quyền thực hiện thủ tục xác định cấp độ an toàn 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 thuê dịch vụ, đơn vị chủ trì thuê dịch vụ lập hồ sơ đề xuất cấp độ; đối với các hệ thống thông tin đang trong giai đoạn triển khai, đơn vị chủ trì triển khai lập hồ sơ đề xuất cấp độ; đối với các hệ thống thông tin đang vận hành, đơn vị vận hành lập hồ sơ đề xuất cấp độ.

2. Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin thực hiện thẩm định, phê duyệt hồ sơ đề xuất cấp độ đối với hệ thống thông tin được đề xuất là cấp độ 1 và cấp độ 2.

3. Đối với hệ thống thông tin được đề xuất là cấp độ 3: Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin thực hiện thẩm định hồ sơ đề xuất cấp độ; chủ quản hệ thống thông tin phê duyệt hồ sơ đề xuất cấp độ.

4. Đối với các hệ thống thông tin được đề xuất là cấp độ 4, đơn vị vận hành hệ thống thông tin cần gửi hồ sơ đề xuất cấp độ xin ý kiến chuyên môn của Trung tâm Chuyển đổi số và Thống kê nông nghiệp hoặc đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin; sau khi có ý kiến chuyên môn, đơn vị vận hành hệ thống thông tin tiếp tục xin ý kiến thẩm định của Bộ Thông tin và Truyền thông; khi có ý kiến thẩm định, đơn vị vận hành hệ thống thông tin trình chủ quản hệ thống thông tin phê duyệt hồ sơ đề xuất cấp độ.

5. Đối với các hệ thống thông tin được đề xuất là cấp độ 5, đơn vị vận hành hệ thống thông tin gửi hồ sơ đề xuất cấp độ xin ý kiến chuyên môn của Trung tâm Chuyển đổi số và Thống kê nông nghiệp hoặc đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin; sau khi có ý kiến chuyên môn, đơn vị vận hành hệ thống thông tin tiếp tục xin ý kiến thẩm định của Bộ Thông tin và Truyền thông; khi có ý kiến thẩm định, đơn vị vận hành trình chủ quản hệ thống thôn tin phê duyệt phương án bảo đảm an toàn thông tin đối với hệ thống thông tin cấp độ 5; chủ quản hệ thống thông tin trình Bộ Thông tin và Truyền thông văn bản đề nghị Chính phủ cập nhật hệ thống thông tin vào danh mục Hệ thống thông tin quan trọng quốc gia; Chính phủ phê duyệt hồ sơ đề xuất cấp độ đối với hệ thống thông tin cấp độ 5.

6. Trường hợp đơn vị chuyên trách an toàn thông tin mạng đồng thời là đơn vị vận hành hệ thống thông tin, đơn vị chuyên trách an toàn thông tin mạng trình chủ quản hệ thống thông tin thành lập Hội đồng thẩm định độc lập thực hiện nhiệm vụ thẩm định Hồ sơ đề xuất cấp độ.

Điều 7. Bảo đảm an toàn thông tin mạng đối với hệ thống thông tin, trang thiết bị công nghệ thông tin, thiết bị xử lý thông tin

1. Chủ quản hệ thống thông tin, đơn vị vận hành hệ thống thông tin, đơn vị chuyên trách an toàn thông tin mạng thực hiện các nhiệm vụ sau:

a) Việc xác định cấp độ hệ thống thông tin và xây dựng phương án bảo đảm an toàn hệ thống thông tin theo cấp độ phục vụ mục đích đánh giá an toàn thông tin và bảo đảm an toàn thông tin cho các hệ thống thông tin. Nguyên tắc bảo đảm an toàn thông tin theo cấp độ và nguyên tắc xác định cấp độ căn cứ trên các nguyên tắc quy định tại Điều 4, Điều 5 Nghị định 85/2016/NĐ-CP ngày 01/7/2016.

b) Xác định cấp độ an toàn cho hệ thống thông tin (gồm: lập hồ sơ đề xuất, tổ chức thẩm định, phê duyệt hồ sơ đề xuất cấp độ) theo quy định tại Điều 6 của Quy chế này và triển khai phương án bảo đảm an toàn hệ thống thông tin theo cấp độ theo quy định tại Điều 11 của Quy chế này và hướng dẫn bổ sung của Bộ thông tin và Truyền thông (nếu có).

2. Trách nhiệm bảo đảm an toàn, an ninh thông tin cơ sở hạ tầng mạng, các trang thiết bị công nghệ thông tin, thiết bị xử lý thông tin sử dụng tại đơn vị:

a) Bảo đảm an toàn, an ninh thông tin khi sử dụng máy tính

- 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.

- 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.

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

b) Bảo đảm an toàn thông tin đối với hệ thống mạng máy tính

- Hệ thống mạng nội bộ (LAN) phải được thiết kế phân vùng theo chức năng cơ bản (theo các chính sách an toàn thông tin riêng), bao gồm: vùng mạng người dùng; vùng mạng kết nối hệ thống ra bên ngoài Internet và các mạng khác; vùng mạng máy chủ công cộng; vùng mạng máy chủ nội bộ; vùng mạng máy chủ quản trị. Dữ liệu trao đổi giữa các vùng mạng phải được quản lý, giám sát bởi hệ thống các thiết bị mạng, thiết bị bảo mật.

- Đơn vị trực thuộc Bộ tham gia kết nối, sử dụng hệ thống mạng diện rộng (WAN) của Bộ có trách nhiệm bảo đảm an toàn thông tin đối với hệ thống mạng nội bộ và các thiết bị của mình khi thực hiện kết nối vào mạng diện rộng; thông báo sự cố hoặc các hành vi phá hoại, xâm nhập về Trung tâm Chuyển đổi số và Thống kê nông nghiệp để xử lý; định kỳ sao lưu thông tin, dữ liệu quan trọng;

không được tiết lộ phương thức (tên đăng ký, mật khẩu, tiện ích, tệp tin hỗ trợ và các cách thức khác) để truy nhập vào hệ thống mạng diện rộng cho tổ chức, cá nhân khác; không được tìm cách truy nhập dưới bất cứ hình thức nào vào các khu vực không được phép truy nhập.

- Đơn vị thuộc Bộ phải áp dụng các biện pháp kỹ thuật cần thiết bảo đảm an toàn thông tin trong hoạt động kết nối Internet, tối thiểu đáp ứng các yêu cầu sau: có hệ thống tường lửa và hệ thống bảo vệ truy cập Internet, đáp ứng nhu cầu kết nối đồng thời, hỗ trợ các công nghệ mạng riêng ảo (VPN) thông dụng và có phần cứng mã hóa tích hợp để tăng tốc độ mã hóa dữ liệu và có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ (DDoS); lọc bỏ, không cho phép truy nhập các trang/cổng thông tin có nghi ngờ chứa mã độc hoặc các nội dung không phù hợp.

- Các đường truyền dữ liệu, đường truyền Internet và các hệ thống dây dẫn các mạng LAN, WAN chạy trong các tòa nhà và phòng làm việc phải được lắp đặt trong ống, có nắp che đậy kín, hạn chế khả năng tiếp cận trái phép. Ngắt kết nối cổng Ethernet không sử dụng, đặc biệt là ở khu vực làm việc chung của các cơ quan, đơn vị.

c) Bảo đảm an toàn thông tin đối với trung tâm dữ liệu/phòng máy chủ

- Các thiết bị kết nối mạng, thiết bị bảo mật quan trọng như tường lửa (firewall), thiết bị định tuyến (router), thiết bị chuyển mạch (switch), hệ thống máy chủ, hệ thống lưu trữ SAN, NAS, ... phải được đặt trong trung tâm dữ liệu/phòng máy chủ và phải được thiết lập cơ chế bảo vệ, theo dõi phát hiện xâm nhập và biện pháp kiểm soát truy nhập, kết nối vật lý phù hợp với từng khu vực: 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. Đơn vị chủ quản trung tâm dữ liệu/phòng máy chủ có trách nhiệm xây dựng nội quy hoặc hướng dẫn làm việc khu vực này.

- Trung tâm dữ liệu/phòng máy chủ là khu vực hạn chế tiếp cận chỉ những cá nhân có quyền, nhiệm vụ theo quy định của thủ trưởng đơn vị mới được phép vào trung tâm dữ liệu/phòng máy chủ. Việc vào, ra phòng máy chủ phải được kiểm soát bằng thiết bị bảo vệ (camera, thẻ quẹt, vân tay, sinh trắc học,…).

- Trung tâm dữ liệu/phòng máy chủ phải được trang bị hệ thống lưu điện đủ công suất và duy trì thời gian hoạt động của các máy chủ ít nhất 20 phút khi có sự cố mất điện.

- Trung tâm dữ liệu/phòng máy chủ phải có hệ thống làm mát điều hòa không khí, độ ẩm để đảm bảo môi trường vận hành; hệ thống cảnh báo cháy, hệ thống chữa cháy tự động bằng khí, thiết bị phòng cháy, chữa cháy khẩn cấp; hệ thống cảnh báo hệ thống nguồn điện; hệ thống chống sét lan truyền. Các hệ thống này phải được thiết lập chế độ cảnh báo phù hợp. Đơn vị phải cử cán bộ thường xuyên giám sát thiết bị, hạ tầng của trung tâm dữ liệu/phòng máy chủ.

- Trung tâm Chuyển đổi số và Thống kê nông nghiệp là đơn vị quản lý, vận hành Trung tâm dữ liệu tập trung của Bộ.

Điều 8. Quy định về quản lý tài khoản truy cập

1. Người sử dụng truy cập vào các hệ thống thông tin được cấp và sử dụng tài khoản truy nhập 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, chung một tài khoản truy nhập và 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 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 nhập của người sử dụng thông thường. Tài khoản hệ thống phải được giao đích danh cá nhân làm công tác quản trị. Hạn chế dùng chung tài khoản quản trị.

4. Khi có yêu cầu khóa quyền truy cập hệ thống thông tin của tài khoản đang hoạt động, lãnh đạo đơn vị phải yêu cầu bằng văn bản gửi đơn vị chủ quản hệ thống thông tin. Đơn vị vận hành hệ thống thông tin thực hiện việc khóa quyền truy cập của tài khoản khi có chỉ đạo của đơn vị chủ quản hệ thống thông tin. Đơn vị chủ quản hệ thống thông tin có quyền khóa quyền truy cập của tài khoản trong trường hợp tài khoản đó thực hiện các hành vi tấn công hoặc để xảy ra vấn đề mất an toàn, an ninh thông tin.

5. Quy định về đặt mật khẩu cho tài khoản truy cập của người sử dụng: Việc đặt mật khẩu truy cập, sử dụng, quản trị hệ thống thông tin; truy cập thiết bị lưu khóa bí mật và các tài khoản liên quan phục vụ công việc phải bảo đảm quy tắc:

- 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 đặc biệt trên bàn phím máy tính (' ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; ” ’ <> , . ? /) và dấu cách); không chứa tên tài khoản.

- Mật khẩu phải được đổi ngay sau khi nhận bàn giao từ người khác hoặc có thông báo về sự cố an toàn thông tin, điểm yếu liên quan đến khả năng lộ mật khẩu; mật khẩu phải được đổi tối thiểu 06 tháng một lần đối với tài khoản của người dùng và 03 tháng một lần đối với tài khoản quản trị hệ thống.

- Người sử dụng, người làm công tác quản trị hệ thống có trách nhiệm bảo vệ thông tin tài khoản được cấp, không tiết lộ mật khẩu hoặc đưa cho người khác

phương tiện xác thực tài khoản của mình ngoại trừ các trường hợp: cần xử lý công việc khẩn cấp của đơn vị; cần cung cấp, bàn giao cho đơn vị các thông tin, tài liệu do cá nhân quản lý. Chủ tài khoản phải đổi mật khẩu ngay sau khi kết thúc xử lý các việc này.

Điều 9. Quy định về bảo đảm an toàn thông tin mức ứng dụng

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

2. Phần mềm, ứng dụng phải đáp ứng các yêu cầu 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, SSL, VPN hoặc tương đương khi truy nhập, quản trị phần mềm, ứng dụng từ xa trên môi trường mạng; hạn chế truy cập đến mã nguồn của phần mềm, ứng dụng và phải đặt mã nguồn trong môi trường an toàn 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 03 tháng với những thông tin cơ bản: thời gian, địa chỉ, tài khoản (nếu có), nội dung truy nhập và sử dụng phần mềm, ứng dụng; các lỗi phát sinh trong quá trình hoạt động; thông tin đăng nhập khi quản trị.

a) Phần mềm, ứng dụng 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.

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

Điều 10. Quy định về bảo đảm an toàn thông tin mức dữ liệu

1. Đơn vị phải thực hiện bảo vệ thông tin, dữ liệu liên quan đến hoạt động công vụ, thông tin có nội dung quan trọng, nhạy cảm hoặc không phải là thông tin công khai bằng các biện pháp như: thiết lập phương án bảo đảm tính bí mật, nguyên vẹn và khả dụng của thông tin, dữ liệu; mã hóa thông tin, dữ liệu khi lưu trữ trên hệ thống/thiết bị lưu trữ dữ liệu di động; sử dụng chữ ký số để xác thực và bảo mật thông tin, dữ liệu.

2. Đơn vị cần triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

3. Đơn vị cần bố trí cơ sở hạ tầng riêng (như: máy tính, máy in, máy photocopy, máy scan) không kết nối mạng, đặt mật khẩu, mã hóa dữ liệu và các biện pháp bảo mật khác bảo đảm an toàn, an ninh thông tin để soạn thảo, lưu trữ dữ liệu, thông tin và tài liệu quan trọng ở các mức độ mật, tuyệt mật, tối mật.

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

5. Đối với hoạt động trao đổi thông tin, dữ liệu với bên ngoài, đơn vị và cá nhân thực hiện trao đổi thông tin, dữ liệu ra bên ngoài cam kết và có biện pháp bảo mật thông tin, dữ liệu được trao đổi. Giao dịch trực tuyến phải được truyền đầy đủ, đúng địa chỉ, tránh bị sửa đổi, tiết lộ hoặc nhân bản một cách trái phép; sử dụng các cơ chế xác thực mạnh, chữ ký số khi tham gia giao dịch, sử dụng các giao thức truyền thông an toàn.

Điều 11. 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 ngày 12/8/2022, 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).

Trường hợp không thể đáp ứng đầy đủ yêu cầu của tiêu chuẩn Việt Nam TCVN 11930:2017, đơn vị phải giải trình lý do và đề xuất biện pháp thay thế có tác dụng tương đương (nếu có). Các yêu cầu không đáp ứng phải nằm ngoài các yêu cầu quy định tại Thông tư 12/2022/TT-BTTT ngày 12/8/2022 và chính sách an toàn thông tin mạng của Bộ Nông nghiệp và Phát triển nông thôn.

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. Trung tâm Chuyển đổi số và Thống kê nông nghiệp tổ chức triển khai phương án bảo đảm an toàn thông tin cho các hệ thống thông tin dùng chung của

Bộ do Trung tâm quản lý, vận hành và các hệ thống thông tin của Thanh tra Bộ, các Vụ thuộc Bộ (nếu có yêu cầu), chịu trách nhiệm giám sát việc triển khai các phương án bảo đảm an toàn thông tin đã được phê duyệt.

Điều 12. Giám sát an toàn thông tin mạng

1. Các hệ thống thông tin phải được thực hiện giám sát an toàn thông tin.

2. Chủ quản hệ thống thông tin chỉ đạo việc giám sát đối với các hệ thống thông tin thuộc phạm vi quản lý, phối hợp với Trung tâm Chuyển đổi số và Thống kê nông nghiệp và các đơn vị chức năng của Bộ Thông tin và Truyền thông giám sát theo quy định.

3. Các hệ thống thông tin bắt buộc phải có chức năng ghi và lưu trữ nhật ký về hoạt động của hệ thống và người sử dụng hệ thống thông tin. Thực hiện việc bảo vệ các chức năng ghi nhật ký và thông tin nhật ký, chống giả mạo, sửa đổi, phá hủy và truy cập trái phép.

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 ngày 15/11/2017.

5. Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia phối hợp với Cục An ninh mạng và Phòng chống tội phạm công nghệ cao – Bộ Công an triển khai giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia theo quy định tại khoản 3 Điều 15 Nghị định số 53/2022/NĐ-CP.

6. Các đơn vị thuộc Bộ cử 01 lãnh đạo đơn vị và 01 cán bộ phụ trách an toàn thông tin làm đầu mối giám sát an toàn thông tin mạng để tiếp nhận cảnh báo, cung cấp, trao đổi, chia sẻ thông tin với Trung tâm Chuyển đổi số và Thống kê nông nghiệp trong các hoạt động giám sát an toàn thông tin của đơn vị và của Bộ.

Điều 13. Kiểm tra, đánh giá an toàn thông tin mạng

1. Các hệ thống thông tin phải được kiểm tra, đánh giá an toàn thông tin.

2. 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.

3. Quy định chung, nội dung, hình thức của hoạt động kiểm tra, đánh giá theo quy định tại Điều 11 Điều 12 Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022.

4. Trung tâm Chuyển đổi số và Thống kê nông nghiệp thực hiện việc kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ theo quy định tại Điều 12 Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 và phương án bảo đảm an toàn cho các hệ thống thông tin tại Bộ. Nội dung đánh giá là cơ sở để điều chỉnh phương án bảo đảm an toàn thông tin

cho phù hợp.

Điều 14. Ứng cứu sự cố an toàn thông tin mạng

1. Ban chỉ đạo, Cơ quan thường trực ứng cứu sự cố an toàn thông tin mạng của Bộ:

a) Ban Chỉ đạo Chuyển đổi số của Bộ theo Quyết định số 3133/QĐ-BNN-TCCB ngày 01/8/2023 đảm nhiệm chức năng Ban chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng của Bộ Nông nghiệp và Phát triển nông thôn. Trách nhiệm và quyền hạn của Ban Chỉ đạo được quy định tại Khoản 2, Điều 5 Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017.

b) Trung tâm Chuyển đổi số và Thống kê nông nghiệp là Cơ quan thường trực Đội ứng cứu sự cố an toàn thông tin mạng của Bộ theo quy định tại Điều 4 Quyết định số 5135/QĐ-BNN-TH ngày 30/12/2022. Thành viên Đội ứng cứu sự cố an toàn thông tin mạng của Bộ theo Quyết định số 5135/QĐ-BNN-TH ngày 30/12/2022 tại các đơn vị trực thuộc Bộ đảm nhiệm vai trò đầu mối về ứng cứu sự cố an toàn thông tin mạng trong phạm vi quản lý công nghệ thông tin của đơn vị. Đơn vị chuyên trách, cơ quan thường trực về ứng cứu sự cố an toàn thông tin mạng thực hiện trách nhiệm quy định tại khoản 2 Điều 6 Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017.

c) Trung tâm Chuyển đổi số và Thống kê nông nghiệp rà soát trình Bộ kiện toàn Đội ứng cứu an toàn thông tin mạng của Bộ và tổ chức ứng cứu sự cố trong phạm vi của Bộ quản lý. Các đơn vị thuộc Bộ rà soát, cử cán bộ chuyên trách tham gia Đội ứng cứu sự cố an toàn thông tin mạng của Bộ theo đề nghị của Trung tâm Chuyển đổi số và Thống kê nông nghiệp.

2. Kế hoạch ứng phó sự cố an toàn thông tin 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 ngày 16/03/2017 (bao gồm các điều chỉnh do Bộ Thông tin và Truyền thông ban hành nếu có) 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 Trung tâm Chuyển đổi số và Thống kê nông nghiệp, Vụ 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 Trung tâm Chuyển đổi số và Thống kê nông nghiệp tổng hợp thành kế hoạch chung của Bộ. Trung tâm Trung tâm Chuyển đổi số và Thống kê nông nghiệp 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 toàn, an ninh thông tin năm tiếp theo.

3. Quy trình ứng cứu sự cố an toàn thông tin mạng của Bộ:

a) Các Cơ quan, đơn vị, tổ chức, cá nhân khi phát hiện dấu hiệu tấn công hoặc sự cố an toàn thông tin mạng cần nhanh chóng báo cho đơn vị vận hành hệ thống thông tin, đơn vị chủ quản hệ thống thông tin, Trung tâm Trung tâm Chuyển đổi số và Thống kê nông nghiệp. Trung tâm Trung tâm Chuyển đổi số và Thống kê nông nghiệp có trách nhiệm cập nhật, công khai thông tin liên lạc, đường dây nóng đầu mối tiếp nhận thông tin sự cố của Bộ và của các đơn vị trực thuộc Bộ trên Cổng thông tin điện tử của Bộ.

b) Khi xảy ra sự cố an toàn thông tin mạng thuộc loại hình tấn công mạng, đơn vị vận hành hệ thống thông tin thực hiện báo cáo theo quy định tại Điểm a Khoản 1 Điều 11 Quyết định 05/2017/QĐ-TTg ngày 16/3/2017 và Điều 9 Thông tư 20/2017/TT-BTTTT ngày 12/9/2017, đồng thời báo cáo Trung tâm Chuyển đổi số và Thống kê nông nghiệp để tổng hợp, báo cáo Ban Chỉ đạo Chuyển đổi số của Bộ. Trách nhiệm của các đơn vị khi phát hiện, tiếp nhận xác minh, xử lý ban đầu và phân loại sự cố an toàn thông tin mạng theo quy định tại Điều 12 Quyết định 05/2017/QĐ-TTg ngày 16/3/2017 và Điều 10 Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017.

c) Quy trình ứng cứu sự cố an toàn thông tin mạng theo quy định tại Điều 13, Điều 14 Quyết định 05/2017/QĐ-TTg ngày 16/3/2017 và Điều 11 Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017.

4. Diễn tập ứng cứu sự cố an toàn thông tin 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) Trung tâm Chuyển đổi số và Thống kê nông nghiệp chủ trì, phối hợp với các đơn vị thuộc Bộ tham gia các cuộc diễn tập quốc gia, quốc tế do Cơ quan điều phối quốc gia, Bộ Thông tin và Truyền thông tổ chức và 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 ngày 25/10/2017 của Thủ tướng Chính phủ.

Điều 15. Đào tạo, bồi dưỡng nghiệp vụ, tuyên truyền, phổ biến nâng cao nhận thức về an toàn thông tin mạng

1. Các đơn vị trực thuộc Bộ xác định nhu cầu về đào tạo nguồn nhân lực bảo đảm an toàn thông tin tại đơn vị mình gửi Trung tâm Chuyển đổi số và Thống kê nông nghiệp. Trung tâm Chuyển đổi số và Thống kê nông nghiệp tổng hợp, xây dựng 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 cán bộ, công chức, viên chức và người lao động của Bộ và thực hiện tổ chức đào tạo theo kế hoạch đã phê duyệt.

2. Các đơn vị thuộc Bộ tổ chức đào tạo, bồi dưỡng nghiệp vụ về an toàn thông tin cho cán bộ công nghệ thông tin, cán bộ chuyên trách an toàn thông tin mạng các đơn vị trực thuộc; đào tạo cơ bản về an toàn thông tin cho cán bộ quản

lý, người sử dụng máy tính thuộc đơn vị.

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 toàn, an ninh thông tin mạng đến toàn thể bộ cán bộ, công chức, viên chức và người lao động tại đơn vị.

4. Trung tâm Chuyển đổi số và Thống kê nông nghiệp xây dựng trình Bộ kế hoạch tuyên truyền, phổ biến nâng cao nhận thức về an toàn, an ninh thông tin mạng tại Bộ và thực hiện các nội dung theo kế hoạch đã được phê duyệt.

Điều 16. Chế độ báo cáo an toàn, an ninh thông tin mạng

1. Báo cáo định kỳ:

a) Báo cáo an toàn thông tin định kỳ hàng năm gồm các nội dung quy định tại Điều 14 Thông tư 12/2022/TT-BTTTT ngày 12/8/2022.

b) Báo cáo hoạt động giám sát của chủ quản hệ thống thông tin định kỳ 6 tháng theo mẫu tại Phụ lục 2 Thông tư 31/2017/TT-BTTTT ngày 15/11/2017.

2. Báo cáo đột xuất: Báo cáo về công tác khắc phục mã độc, lỗ hổng, điểm yếu, triển khai cảnh báo an toàn thông tin và các báo cáo đột xuất khác theo yêu cầu của đơn vị chuyên trách về an toàn thông tin của Bộ hoặc yêu cầu của Lãnh đạo Bộ và của Cơ quan chức năng.

3. Trách nhiệm lập, phê duyệt báo cáo

a) Các đơn vị thuộc Bộ chịu trách nhiệm:

- Lập báo cáo an toàn thông tin mạng theo quy định tại điểm a khoản 1 điều này, gửi Trung tâm Chuyển đổi số và Thống kê nông nghiệp 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 Trung tâm Chuyển đổi số và Thống kê nông nghiệp trước ngày 20 tháng 6 và 20 tháng 12 hàng năm.

- Báo cáo đột xuất theo hướng dẫn của Trung tâm Chuyển đổi số và Thống kê nông nghiệp, Lãnh đạo Bộ và của Cơ quan chức năng.

b) Trung tâm Chuyển đổi số và Thống kê nông nghiệp 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 toàn thông tin.

Chương III
TỔ CHỨC THỰC HIỆN

Điều 17. Kinh phí thực hiện

- Kinh phí đảm bảo an toàn thông tin mạng, an ninh mạng được đảm bảo từ nguồn chi thường xuyên hàng năm, hoặc lồng ghép, tích hợp với các chương trình, dự án, nhiệm vụ sử dụng nguồn ngân sách nhà nước và các nguồn kinh phí hợp pháp

khác.

- Căn cứ vào kế hoạch hàng năm, các đơn vị thuộc Bộ có trách nhiệm xây dựng kế hoạch, đề xuất dự toán cho các hoạt động bảo đảm an toàn thông tin mạng gửi Trung tâm Chuyển đổi số và Thống kê nông nghiệp tổng hợp gửi Vụ Kế hoạch, Vụ Tài chính xem xét, thẩm định, trình Bộ.

Điều 18. Trách nhiệm của Trung tâm Chuyển đổi số và Thống kê nông nghiệp

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 toàn thông tin mạng và an ninh mạng.

3. Tổ chức triển khai thực hiện Quy chế tại trụ sở cơ quan Bộ Nông nghiệp và Phát triển nông thôn.

4. Xây dựng kế hoạch, báo cáo về an toàn thông tin mạng, an ninh mạng của Bộ Nông nghiệp và Phát triển nông thôn.

5. Bảo đảm an toàn thông tin cho hệ thống mạng nội bộ, hệ thống an toàn, an ninh mạng, các hệ thống thông tin, cơ sở dữ liệu dùng chung của Bộ, các hệ thống thông tin do Thanh tra Bộ, các Vụ thuộc Bộ làm chủ quản (nếu có yêu cầu) và các hệ thống thông tin khác theo quyết định của Bộ trưởng.

Điều 19. 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 Trung tâm Chuyển đổi số và Thống kê nông nghiệp tổng hợp, báo cáo Bộ.

4. Xây dựng, triển khai Quy chế bảo đảm an toàn thông tin 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, hệ thống an toàn, an ninh mạng, các hệ thống thông tin, cơ sở dữ liệu theo Khoản 2 Điều 5 của Quy chế này.

6. Đối với Khối Vụ, Thanh tra Bộ: Phối hợp với Trung tâm Chuyển đổi số và Thống kê nông nghiệp bảo đảm an toàn thông tin 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 20. Trách nhiệm của đơn vị chuyên trách về an toàn thông tin

1. Thực hiện trách nhiệm của đơn vị chuyên trách về an toàn thông tin theo quy định tại Quy chế này và các nhiệm vụ do chủ quản hệ thống thông tin phân công.

2. Phối hợp chặt chẽ với các bộ phận kỹ thuật thuộc đơn vị vận hành hệ

thống thông tin trong việc bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

Điều 21. 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 toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

Điều 22. 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 toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

Điều 23. 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 cán bộ, 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 mật thuộc phạm vi quản lý của đơn vị do không tổ chức, chỉ đạo, kiểm tra cán bộ của đơn vị thực hiện đúng quy định.

2. Cán bộ, công chức, viên chức, người lao động của Bộ Nông nghiệp và Phát triển nông thôn, các đơn vị thuộc Bộ và các đơn vị khác thuộc đối tượng áp dụng của quy định có trách nhiệm: tuân thủ Quy chế; thông báo các vấn đề bất thường liên quan tới an toàn thông tin mạng, an ninh mạng cho đơn vị, bộ phận chuyên trách về an toàn thông tin mạng của đơn vị; chịu trách nhiệm trước pháp luật và Lãnh đạo đơn vị về các vi phạm, thất thoát dữ liệu mật của ngành nông nghiệp và phát triển nông thôn do không tuân thủ Quy chế.

Điều 24. Trách nhiệm thi hành

1. Thủ trưởng các đơn vị trực thuộc Bộ có trách nhiệm phổ biến, quán triệt đến toàn bộ cán 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 thuộc Bộ phản ảnh về Trung tâm Chuyển đổi số và Thống kê nông nghiệp để tổng hợp, trình Bộ trưởng xem xét, sửa đổi, bổ sung quy chế./.