

Số: 63/QĐ-TTNS

Hà Nội, ngày 18 tháng 7 năm 2025

QUYẾT ĐỊNH

**Ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng của
Trung tâm Quốc Gia Nước sạch và Vệ sinh môi trường nông thôn**

Giám đốc Trung tâm Quốc gia Nước sạch và Vệ sinh môi trường nông thôn

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

Căn cứ Luật An ninh mạng ngày 12/6/2018;

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

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 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 17/4/2023 của Chính phủ về bảo vệ dữ liệu cá nhân;

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

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 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 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 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 12/9/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

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

Căn cứ Quyết định số 315/QĐ-BNNMT ngày 01/3/2025 của Bộ trưởng Bộ Nông nghiệp và Môi trường quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Cục Quản lý và Xây dựng công trình thủy lợi;

Căn cứ Quyết định số 1921/QĐ-BNNMT ngày 05/06/2025 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;

Căn cứ Quyết định số 29/QĐ-TTNS ngày 24/6/2025 của Giám đốc Trung tâm Quốc gia Nước sạch và Vệ sinh môi trường nông thôn về việc ban hành Quy chế làm việc của Trung tâm Quốc gia Nước sạch và Vệ sinh môi trường nông thôn;

Theo đề nghị của Trưởng phòng Phòng Hành chính Tổng hợp.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng của Trung tâm Quốc gia Nước sạch và Vệ sinh môi trường nông thôn.

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

Điều 3. Trưởng phòng Phòng Hành chính, Tổng hợp; Trưởng các đơn vị; toàn thể viên chức và người lao động Trung tâm Quốc gia Nước sạch và Vệ sinh môi trường nông thôn chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:

- Như Điều 3;
- Lưu: VT, HC.

GIÁM ĐỐC



Nguyễn Thành Luân

QUY CHẾ
BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG, AN NINH MẠNG CỦA
TRUNG TÂM QUỐC GIA NƯỚC SẠCH VÀ VỆ SINH MÔI TRƯỜNG
NÔNG THÔN

(Kèm theo Quyết định số: 63/QĐ-TTNS ngày 18 / 7 /2025
của Giám đốc Trung tâm Quốc gia Nước sạch và Vệ sinh môi trường 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 hoạt động ứng dụng công nghệ thông tin, chính phủ điện tử, chính phủ số, chuyển đổi số, cơ sở dữ liệu ngành của Trung tâm Quốc gia Nước sạch và Vệ sinh môi trường nông thôn.

2. Đối tượng áp dụng:

a) Các đơn vị trực thuộc Trung tâm Quốc gia Nước sạch và Vệ sinh môi trường nông thôn (sau đây gọi là đơn vị thuộc Trung tâm); Viên chức và người lao động thuộc các đơn vị thuộc Trung tâm; các tổ chức, cá nhân có quan hệ làm việc với Trung tâm.

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

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 cho các đơn vị thuộc Trung tâm.

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, viên chức, người lao động tại các cơ quan, đơn vị thuộc Cục 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.

Điều 3. Mục tiêu và nguyên tắc bảo đảm an toàn, an ninh thông tin mạng

1. Mục tiêu bảo đảm an toàn thông tin, 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 các Hệ thống thông tin thuộc lĩnh vực: Nước sạch, Vệ sinh môi trường nông thôn,...

2. Nguyên tắc bảo đảm an toàn, an ninh thông tin mạng

a) Đơn vị, cá nhân thuộc đối tượng áp dụng Quy chế này có trách nhiệm bảo đảm an toàn thông tin, an ninh mạng trong phạm vi xử lý công việc của mình theo quy định của pháp luật, hướng dẫn của cơ quan, đơn vị có thẩm quyền và các quy định tại Quy chế này bao gồm việc quản lý an toàn tài khoản, mật khẩu, chứng thư số, dữ liệu được giao.

b) Bảo đảm an toàn thông tin, an ninh mạng được thực hiện xuyên suốt, toàn trình trong khâu mua sắm, nâng cấp, vận hành, bảo trì và ngừng sử dụng hạ tầng, hệ thống thông tin, phần mềm, dữ liệu.

c) 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.

d) 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.

đ) Trường hợp có 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.

e) Thông tin thuộc Danh mục bí mật nhà nước được bảo vệ theo quy định của pháp luật về bảo vệ bí mật nhà nước.

f) An toàn thông tin mạng phải gắn liền và hỗ trợ các hoạt động ứng dụng công nghệ thông tin, chính phủ điện tử, chính phủ số, chuyển đổi số của Trung tâm; hỗ trợ việc sử dụng trang thiết bị công nghệ thông tin, thiết bị xử lý thông tin để xử lý công việc của người dùng.

g) 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.

h) Người dùng 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 các văn bản pháp luật có liên quan.

2. Tấn công, vô hiệu hóa trái phép làm mất tác dụng của biện pháp bảo vệ ATTT cho hệ thống thông tin; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để cố ý vượt qua biện pháp kiểm soát truy cập, tấn công, chiếm quyền điều khiển trái phép đối với hệ thống thông tin.

3. Phát tán thông tin độc hại dưới mọi hình thức:

- Phát tán thư rác, tin nhắn rác, phần mềm độc hại.
- Sử dụng trái phép công cụ ẩn danh, proxy, VPN nhằm che giấu nguồn gốc, truy cập bất hợp pháp vào hệ thống của Trung tâm.

4. Làm thay đổi hệ thống mạng: tự ý lắp đặt thêm bộ chuyển mạch (switch), lắp đặt thêm mạng không dây, cấu hình địa chỉ IP...Cấm lưu trữ, đưa lên mạng hoặc trao đổi các thông tin sau:

- Thông tin chưa được cấp có thẩm quyền công bố.
- Thông tin thuộc danh mục thông tin mật do pháp luật hiện hành quy định.
- Thông tin và các dịch vụ thông tin trái với quy định của pháp luật hiện hành như: Gây ảnh hưởng đến an ninh quốc gia; Xuyên tạc, tuyên truyền chống đối chính sách và pháp luật của Nhà nước; Có nội dung kích động bạo lực, tuyên truyền chiến tranh xâm lược, gây hận thù giữa các dân tộc và nhân dân các nước, truyền bá tư tưởng phản động; Có ảnh hưởng đến văn hoá xã hội và thuần phong mỹ tục; Giả

mạo nguồn gốc của thông tin; Có ảnh hưởng xấu đến đời tư người khác: quấy rối cá nhân, xúc phạm danh dự, vu khống, xúc phạm đến nhân phẩm người khác.

5. Chiếm đoạt, sử dụng trái phép dữ liệu và công cụ bảo mật, bao gồm:

- Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã, chứng thư số hoặc dữ liệu của đơn vị, cá nhân khác.

- Cài đặt, sử dụng phần mềm, công cụ dò quét mật khẩu, thu thập trái phép thông tin nhận dạng cá nhân, dữ liệu nghiệp vụ.

Chương II

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

Điều 5. Phân công thực hiện về bảo đảm an toàn thông tin mạng cho các hệ thống thông tin của Trung tâm Quốc gia Nước sạch và Vệ sinh môi trường nông thôn theo quy định của pháp luật

1. Phòng Hành chính, Tổng hợp – Trung tâm Quốc gia Nước sạch và Vệ sinh môi trường nông thôn chủ trì phụ trách quản lý trang tin điện tử của Trung tâm.

Chịu trách nhiệm về cấp độ hệ thống trang thông tin của Trung tâm theo quy định tại Khoản 2, Điều 20, Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ và Quy chế an toàn thông tin mạng và An ninh mạng Bộ Nông nghiệp và Môi trường (*Quyết định số 1921/QĐ-BNNMT ngày 05/6/2025*)

2. Các đơn vị thuộc Trung tâm phụ trách nội dung, cơ sở dữ liệu, phần mềm do các đơn vị thực hiện chủ trì theo chức năng, nhiệm vụ đã được giao.

Chịu trách nhiệm về cấp độ hệ thống trang thông tin, cơ sở dữ liệu, phần mềm do các đơn vị chủ trì xây dựng theo quy định tại Khoản 2, Điều 20, Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ và Quy chế an toàn thông tin mạng và An ninh mạng Bộ Nông nghiệp và Môi trường (*Quyết định số 1921/QĐ-BNNMT ngày 05/6/2025*).

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

1. 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.

2. 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.

3. 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.

2. Đơn vị 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.

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. Trong quá trình vận hành hệ thống thông tin, đơn vị quản lý trực tiếp 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;

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

4. Hệ thống thông tin quản lý, hệ thống cơ sở dữ liệu, hệ thống máy chủ phải có chức năng tự động ghi nhật ký (trong khoảng thời gian nhất định, tối thiểu là 03 tháng) quá trình đăng nhập vào hệ thống, các thao tác cấu hình hệ thống và các thông tin liên quan về an toàn thông tin để phục vụ công tác khắc phục sự cố và điều tra về an toàn thông tin khi xảy ra.

5. Các Hệ thống thông tin phải được trang bị các giải pháp kỹ thuật, công nghệ bảo mật, có chức năng giám sát, kiểm soát và phát hiện, ngăn chặn truy cập trái phép.

6. Các đơn vị 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 thông tin đối với dữ liệu

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

ngày 05 tháng 6 năm 2025 của Bộ trưởng Bộ Nông nghiệp và Môi trường về việc ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Bộ Nông nghiệp và Môi trường.

Điều 10. Quản lý an toàn, an ninh thông tin đối với hạ tầng mạng, thiết bị số

1. Hạ tầng mạng (hệ thống mạng nội bộ, kết nối mạng Internet)

- Hệ thống mạng của Trung tâm là hệ thống mạng độc lập không tham gia, kết nối trực tiếp vào hệ thống mạng máy tính của Cục, Bộ.

- Thực hiện theo Điều 10 Quy chế bảo đảm an toàn, an ninh thông tin mạng Bộ Nông nghiệp và Môi trường tại Quyết định số 1921/QĐ-BNNMT ngày 05 tháng 6 năm 2025 của Bộ trưởng Bộ Nông nghiệp và Môi trường về việc ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Bộ Nông nghiệp và Môi trường.

2. Thiết bị số

- Sử dụng hệ điều hành được hỗ trợ bản vá lỗ hổng bảo mật. Chỉ cài đặt tiện ích thiết yếu được cung cấp kèm theo hệ điều hành và các phần mềm phục vụ công việc, có bản quyền hoặc được các cơ quan chức năng đánh giá, xác nhận an toàn. Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính phải tắt máy và báo trực tiếp cho bộ phận chuyên trách về công nghệ thông tin để được xử lý kịp thời.

- Thiết bị số soạn thảo văn bản chứa nội dung bí mật nhà nước, lưu trữ bí mật nhà nước: Không kết nối vào mạng Internet, mạng nội bộ, mạng không dây, mạng viễn thông.

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

- Có trách nhiệm bảo mật tài khoản truy cập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác;

- 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;

Điều 11. Quản lý an toàn, an ninh thông tin 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.

2. Cá nhân được cấp hoặc giao tài khoản chịu trách nhiệm về các hành vi của tài khoản được ghi nhận trên thiết bị xử lý thông tin, hệ thống thông tin.

3. Đơn vị vận hành hệ thống thông tin thường xuyên rà soát các tài khoản truy cập hệ thống đang hoạt động, phát hiện và thu hồi các tài khoản không sử dụng hoặc không hợp lệ, điều chỉnh thông tin tài khoản chưa phản ánh chính xác thông tin thực tế tại thời điểm rà soát.

Điều 12. Giám sát an toàn thông tin mạng

1. Các hệ thống thông tin phải được thực hiện giám sát an toàn thông tin.
2. 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.
3. Nguyên tắc, yêu cầu, nội dung, phương thức, hệ thống kỹ thuật phục vụ công tác giám sát thực hiện theo quy định tại Thông tư số 31/2017/TT-BTTTT.

Điều 13. 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 trước ngày 15 tháng 11 gồm các nội dung quy định tại Điều 13, Điều 14 Thông tư 12/2022/TT-BTTTT.
 - b) Báo cáo hoạt động giám sát của chủ quản hệ thống thông tin định kỳ 6 tháng trước ngày 15 tháng 6 và 15 tháng 12 hàng năm theo mẫu tại Phụ lục 2 Thông tư 31/2017/TT-BTTTT.
2. Báo cáo đột xuất: Báo cáo về công tác khắc phục mã độc, lỗ hổng, điểm yếu, triển khai cảnh báo an toàn thông tin và các báo cáo đột xuất khác theo yêu cầu của các cơ quan quản lý nhà nước về an toàn thông tin.
3. Trách nhiệm lập, phê duyệt báo cáo
 - a) Các đơn vị thuộc Trung tâm có trách nhiệm lập báo cáo định kỳ, báo cáo đột xuất theo yêu cầu theo nội dung quy định tại khoản 1 Điều này gửi Phòng Hành chính, Tổng hợp.
 - b) Phòng Hành chính, Tổng hợp chịu trách nhiệm tập hợp, tổng hợp báo cáo của các đơn vị, trình Lãnh đạo Trung tâm phê duyệt, gửi Lãnh đạo Cục Quản lý và Xây dựng công trình thủy lợi và các cơ quan quản lý nhà nước về an toàn thông tin.

Chương III TỔ CHỨC THỰC HIỆN

Điều 14. Trách nhiệm của Trưởng các đơn vị trực thuộc Trung tâm Quốc gia Nước sạch và Vệ sinh môi trường nông thôn

Có trách nhiệm phổ biến, quán triệt nội dung Quy chế này đến toàn thể viên chức, người lao động trong đơn vị và nghiêm túc tổ chức triển khai thực hiện. Chịu

trách nhiệm về đảm bảo an toàn thông tin mạng, an ninh mạng đối với cơ sở dữ liệu, các phần mềm do đơn vị phụ trách theo chức năng, nhiệm vụ được giao, báo cáo tình hình an toàn, an ninh mạng theo quy định.

Điều 15. Trách nhiệm của Phòng Hành chính, Tổng hợp

- Giao Phòng Hành chính, Tổng hợp là đơn vị chuyên trách về an toàn thông tin của Trung tâm phù hợp với quy định tại điểm b khoản 3 Điều 5 Quyết định số 1921/QĐ-BNNMT ngày 05/06/2025 của Bộ Nông nghiệp và Môi trường; viên chức quản trị công nghệ thông tin hệ thống mạng nội bộ của Trung tâm có trách nhiệm bảo đảm an ninh mạng của Trung tâm, hướng dẫn và phối hợp với các phòng, đơn vị trong Trung tâm triển khai các biện pháp đảm bảo an toàn thông tin, an ninh mạng đối với cơ sở dữ liệu, phần mềm do các đơn vị được Trung tâm giao chủ trì xây dựng, vận hành.

- Tham mưu cho Giám đốc về công tác bảo đảm ATTT tại Trung tâm và chịu trách nhiệm trước Giám đốc trong việc đảm bảo ATTT cho các hệ thống CNTT được giao phụ trách.

- Hàng năm phối hợp với các đơn vị xây dựng kế hoạch, đề xuất nguồn kinh phí để triển khai công tác ATTT trong hoạt động ứng dụng CNTT của Trung tâm.

- Phối hợp với các phòng, đơn vị thuộc Trung tâm triển khai các nhiệm vụ ATTT. Xây dựng và triển khai các chương trình đào tạo, hội nghị tuyên truyền ATTT.

- Thông báo đến các phòng biết và có biện pháp phòng ngừa, ngăn chặn các nguy cơ mất ATTT do virus, phần mềm gián điệp,... gây ra.

- Chủ trì, phối hợp với các cơ quan liên quan thành lập đoàn kiểm tra, tiến hành kiểm tra định kỳ hoặc đột xuất khi phát hiện có các dấu hiệu, hành vi vi phạm ATTT.

- Hàng năm, tổng hợp và báo cáo Giám đốc tình hình triển khai ATTT.

Điều 16. Trách nhiệm của bộ phận Kế toán - Phòng Hành chính, Tổng hợp

Phối hợp với Lãnh đạo Phòng Hành chính, Tổng hợp và các phòng, đơn vị có liên quan đề xuất nguồn kinh phí cho công tác đảm bảo an toàn thông tin mạng, an ninh mạng của Trung tâm; đảm bảo an toàn thông tin mạng, an ninh mạng đối với cơ sở dữ liệu, phần mềm do Phòng, đơn vị phụ trách theo chức năng, nhiệm vụ được giao.

Điều 17. Trách nhiệm của viên chức

Viên chức, người lao động của Trung tâm, các đơn vị thuộc Trung tâm thuộc đối tượng áp dụng của Quy chế có trách nhiệm: tuân thủ Quy chế; thông báo các

dấu hiệu mất an toàn thông tin cho đơn vị, bộ phận chuyên trách về an toàn thông tin mạng của Trung tâm; chịu trách nhiệm trước pháp luật và Lãnh đạo Trung tâm về các vi phạm, thất thoát dữ liệu quan trọng hoặc dữ liệu mật do không tuân thủ Quy chế.

Điều 18. Điều khoản thi hành

- Quy chế này có hiệu lực kể từ ngày ký.
- Trong quá trình thực hiện, nếu các văn bản viện dẫn làm căn cứ để xây dựng Quy chế này thay đổi thì áp dụng theo văn bản mới hoặc có các vấn đề vướng mắc, phát sinh, các đơn vị kịp thời thông báo về Phòng Hành chính, Tổng hợp để tổng hợp trình Giám đốc xem xét, điều chỉnh cho phù hợp./.

**TRUNG TÂM QUỐC GIA NƯỚC SẠCH
VÀ VỆ SINH MÔI TRƯỜNG NÔNG THÔN**



Nguyễn Thành Luân