SỞ NÔNG NGHIỆP & PTNT HÀ NAM
CHI CỤC CHẤT LƯỢNG, CHẾ BIẾN VÀ PHÁT TRIỂN THỊ TRƯỜNG

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

Số: 04 /QĐ-CLCB&PTTT

Hà Nam, ngày 22 tháng 01 năm 2025

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn, an ninh mạng Hệ thống cơ sở dữ liệu truy xuất nguồn gốc nông lâm thủy sản thực phẩm tỉnh Hà Nam

CHI CỤC TRƯỞNG
CHI CỤC CHẤT LƯỢNG, CHẾ BIẾN VÀ PHÁT TRIỂN THỊ TRƯỜNG

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19/6/2015;

Căn cứ Luật sửa đổi, bổ sung một số điều của Luật Tổ chức Chính phủ và Luật Tổ chức chính quyền địa phương ngày 22/11/2019;

Căn cứ Luật Công nghệ thông tin ngày 29/6/2006;

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 số 29/2018/QH14 ngày 15/11/2018; 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 các Nghị định của Chính phủ: số 142/2016/NĐ-CP ngày 01/7/2016 về ngăn chặn xung đột thông tin trên mạng; số 53/2022/NĐ-CP ngày 15/8/2022 về việc quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Chỉ thị số 02/CT-TTg ngày 26/4/2022 của Thủ tướng Chính phủ về phát triển Chính phủ điện tử hướng tới Chính phủ số, thúc đẩy chuyển đổi số quốc gia;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 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 15/11/2017 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 12/8/2022 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 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

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 tiêu chuẩn Quốc gia TCVN 11930:2017 về công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 56/2023/QĐ-UBND ngày 28/11/2023 của Ủy ban nhân dân tỉnh Hà Nam về việc đổi tên Chi cục Quản lý chất lượng Nông, Lâm sản và Thủy sản thành Chi cục Chất lượng, Chế biến và Phát triển thị trường trực thuộc Sở Nông nghiệp và Phát triển nông thôn và quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Chi cục;

Theo đề nghị của Trưởng phòng Nghiệp vụ,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn, an ninh mạng Hệ thống cơ sở dữ liệu truy xuất nguồn gốc nông lâm thủy sản thực phẩm tỉnh Hà Nam.

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

Điều 3. Phòng Hành chính, tổng hợp; Phòng Nghiệp vụ; các công chức Chi cục Chất lượng, Chế biến và Phát triển thị trường và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Lãnh đạo Sở (để b/c);
- Văn phòng Sở (để t/hợp);
- Lãnh đạo Chi cục;
- Như Điều 3;
- Lưu: VT.

CHI CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CHI CỤC CHẤT LƯỢNG CHẾ BIẾN VÀ PHÁT TRIỂN THỊ TRƯỜNG
SỞ NÔNG NGHIỆP VÀ PTNT TỈNH HÀ NAM

Đặng Phan Sơn

SỞ NÔNG NGHIỆP & PTNT HÀ NAM
CHI CỤC CHẤT LƯỢNG, CHẾ BIẾN VÀ PHÁT TRIỂN THỊ TRƯỜNG

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

QUY CHẾ
Bảo đảm an toàn, an ninh mạng Hệ thống cơ sở dữ liệu truy xuất nguồn gốc nông lâm thủy sản thực phẩm tỉnh Hà Nam

(Ban hành kèm theo Quyết định số: /QĐ-CCCBPTTT ngày 22/01/2025 của Chi cục Chất lượng, Chế biến và Phát triển thị 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 quản lý và các biện pháp nhằm bảo đảm an toàn thông tin cho Hệ thống cơ sở dữ liệu truy xuất nguồn gốc nông lâm thủy sản thực phẩm tỉnh Hà Nam (https://hna.check.net.vn) của Chi cục Chất lượng, Chế biến và Phát triển thị trường.

2. Đối tượng áp dụng

Các cơ quan, đơn vị tham gia quản lý, sử dụng hệ thống bao gồm:

a) Cơ quan quản lý nhà nước có hoạt động về quản lý an toàn thực phẩm (sau đây gọi chung là cơ quan quản lý):

- Các phòng chuyên môn trực thuộc Chi cục Chất lượng, Chế biến và Phát triển thị trường.

- Các đơn vị trực thuộc Sở Nông nghiệp & PTNT tỉnh Hà Nam.

- Ủy ban nhân dân các huyện, thị xã, thành phố (sau đây gọi chung là cấp huyện).

- Ủy ban nhân dân các xã, phường, thị trấn (sau đây gọi chung là cấp xã).

b) Các doanh nghiệp, hợp tác xã, tổ hợp tác, hộ gia đình, cá nhân sản xuất kinh doanh thực phẩm nông lâm thủy sản (sau đây gọi chung là cơ sở).

c) Trung tâm Doanh Nghiệp Hội nhập và Phát triển là đơn vị cung cấp hệ thống.

d) Người tiêu dùng.

Điều 2. Giải thích từ ngữ

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

-*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.

- *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.

- *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.

- *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.

- *Hệ thống cơ sở dữ liệu truy xuất nguồn gốc nông lâm thủy sản thực phẩm tỉnh Hà Nam:* Là toàn bộ cấu trúc hệ thống dữ liệu, hệ thống quản trị, quy trình áp dụng và triển khai, hệ thống phần cứng (như máy chủ, máy trạm, đường truyền, hệ thống số hóa thông tin đầu vào, hệ thống lưu trữ và backup dữ liệu,…) cùng hạ tầng bảo quản thiết bị; hệ thống có tên miền, có Module riêng.

- *Cơ sở dữ liệu:* Là thông tin, số liệu được hình thành trong quá trình sử dụng hệ thống.

- *Người sử dụng:* Là người được giao nhiệm vụ quản lý, sử dụng hệ thống thuộc cơ quan được quy định tại khoản 2 Điều 1 Quy chế này được cấp tài khoản để sử dụng trong suốt quá trình cung cấp, cập nhật, khai thác thông tin, quản trị hệ thống.

- *Tài khoản (Account):* Bao gồm tên đăng nhập và mật khẩu để truy cập vào hệ thống. Các loại tài khoản trong Quy chế này gồm:

+ Tài khoản quản trị: Là tài khoản được cấp cho các cơ quan quản lý.

+ Tài khoản vận hành: Là tài khoản được cấp cho các cơ sở.

- *Nguyên tắc truy xuất một bước trước - một bước sau:* Là cơ sở phải lưu giữ thông tin để bảo đảm khả năng nhận diện được cơ sở sản xuất, kinh doanh, công đoạn sản xuất trước và cơ sở sản xuất, kinh doanh, công đoạn sản xuất tiếp theo sau trong quá trình sản xuất, kinh doanh đối với sản phẩm được truy xuất.

- *Vận hành:* Là một chuỗi các hành động liên quan đến việc cập nhật, lưu trữ thông tin trên hệ thống mà người sử dụng cần tuân thủ và thực hiện.

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

1. Mục tiêu bảo đảm an toàn thông tin

Bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy cập, 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 Hệ thống cơ sở dữ liệu truy xuất nguồn gốc nông lâm thủy sản thực phẩm tỉnh Hà Nam

2. Nguyên tắc

a) Cơ quan, tổ chức thuộc đối tượng áp dụng Quy chế này có trách nhiệm bảo đảm an toàn thông tin và hệ thống thông tin 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.

b) Bảo đảm an toàn thông tin là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục trong quá trình:

i. Thu thập, tạo lập, xử lý, truyền tải, lưu trữ và sử dụng thông tin, dữ liệu.

ii. Thiết kế, thiết lập và vận hành, nâng cấp, hủy bỏ hệ thống thông tin.

c) Việc bảo đảm an toàn Hệ thống cơ sở dữ liệu truy xuất nguồn gốc nông lâm thủy sản thực phẩm tỉnh Hà Nam 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.

Điều 4. Những hành vi nghiêm cấm

Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật An toàn thông tin mạng và Điều 8 Luật An ninh mạng.

Điều 5. Phối hợp với những cơ quan/tổ chức có thẩm quyền

1. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin:

Chi cục Chất lượng, Chế biến và Phát triển thị trường là đầu mối liên hệ, phối hợp các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin phục vụ việc bảo đảm an toàn, an ninh mạng cho Hệ thống cơ sở dữ liệu truy xuất nguồn gốc nông lâm thủy sản thực phẩm tỉnh Hà Nam.

Người liên hệ: Ông Tăng Xuân Hòa, Phó Chi cục trưởng Chi cục Chất lượng, Chế biến và Phát triển thị trường;

Số điện thoại: 0983493445; Email: ccqlclnlsvts.nn@hanam.gov.vn

2. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin:

a) Sở Thông tin và Truyền thông tỉnh Hà Nam

Liên hệ: Ông Đỗ Văn Trinh - Phòng Bưu chính - Viễn thông - Công nghệ thông tin

+ Số điện thoại: 0916 862 333

+ Email: Dovantrinh@hanam.gov.vn

b) Cục An toàn thông tin/Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC)

- Người liên hệ/bộ phận: Phòng Ứng cứu sự cố

- Số điện thoại: 0869 100 317

- Email: ir@vncert.vn

- Báo cáo sự cố qua nền tảng điều phối, xử lý sự cố an toàn thông tin mạng quốc gia: https://irlab.vn

- Báo cáo sự cố qua website của VNCERT/CC: https://vncert.vn

c) Trung tâm Doanh nghiệp Hội nhập và Phát triển

- Người liên hệ: Doãn Đình Chúc - Phụ trách kỹ thuật;

Số điện thoại: 0963.056.116; Email: trungtam.ide@gmail.com

Điều 6. Bảo đảm nguồn nhân lực

1. Tuyển dụng/sử dụng: Người được giao sử dụng về an toàn thông tin Hệ thống cơ sở dữ liệu truy xuất nguồn gốc nông lâm thủy sản thực phẩm tỉnh Hà Nam cần có trình độ, chuyên ngành hoặc qua đào tạo, tập huấn về lĩnh vực công nghệ thông tin, an toàn thông tin và phù hợp với vị trí việc làm/tuyển dụng.

2. Trong quá trình làm việc

a) Trách nhiệm bảo đảm an toàn thông tin cho người sử dụng, người được giao quản lý và vận hành hệ thống:

- Với người sử dụng:

Người sử dụng có trách nhiệm đảm bảo an toàn thông tin đối với tài khoản, mật khẩu được giao.

Thường xuyên cập nhật và nghiêm túc chấp hành các quy định về an toàn thông tin, nhằm nâng cao nhận thức về trách nhiệm đảm bảo an toàn thông tin.

- Với người được giao quản lý và vận hành hệ thống:

Người được giao quản lý và vận hành hệ thống phải nghiêm chỉnh chấp hành chế độ bảo mật, an toàn, an ninh thông tin mang; tự bảo quản tài khoản, mật khẩu được giao quản lý

Khi phát hiện nguy cơ mất an toàn thông tin mạng hoặc có dấu hiệu sự cố an toàn thông tin mạng phải báo cáo kịp thời với cấp trên và bộ phần, cán bộ chuyên trách về công nghệ thông tin, an toàn thông tin mạng để xem xét, tham mưu, tổ chức ngăn chặn, xử lý, khắc phục.

b) Định kỳ hàng năm tổ chức hoặc tham gia phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng do đơn vị chức năng tổ chức.

3. Chấm dứt thay đổi công việc

a) Người bị chấm dứt hoặc thay đổi công việc phải bàn giao lại tài khoản, mật khẩu truy cập hệ thống cho người tiếp quản;

b) Bộ phận chuyên trách thực hiện vô hiệu hóa tất cả các quyền truy cập, khai thác thông tin, quản trị hệ thống sau khi cán bộ thôi việc.

Chương II
BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ THIẾT KẾ, XÂY DỰNG HỆ THỐNG

Điều 7. Thiết kế an toàn hệ thống thông tin

1. Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin và thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

2. Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

3. Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ của hệ thống thông tin thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

4. Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin của hệ thống thông tin thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

5. Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống, báo cáo Lãnh đạo quyết định trước khi thực hiện thay đổi.

Điều 8. Phát triển phần mềm

Yêu cầu có biên bản, hợp đồng và các cam kết đối với bên đơn vị cung cấp hệ thống các nội dung liên quan đến việc nâng cấp, mở rộng các tính năng của hệ thống.

Điều 9. Thử nghiệm và nghiệm thu hệ thống

1. Bên triển khai xây dựng kế hoạch, nội dung thử nghiệm hệ thống trước khi thực hiện thử nghiệm và nghiệm thu hệ thống.

2. Đơn vị vận hành thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác theo phương án thiết kế được phê duyệt trong Hồ sơ đề xuất cấp độ.

3. Bộ phận chuyên trách và bên triển khai hệ thống xây dựng kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống, trình Lãnh đạo đơn vị phê duyệt trước khi đưa hệ thống vào vận hành, khai thác.

4. Bộ phận chuyên trách phối hợp với bên triển khai hệ thống thực hiện thử nghiệm và nghiệm thu hệ thống, trước khi đưa vào vận hành, khai thác.

Chương III
BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ VẬN HÀNH HỆ THỐNG

Điều 10. Quản lý an toàn mạng

1. Hoạt động của hệ thống phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của hệ thống.

2. Toàn bộ cấu hình hệ thống phải được sao lưu, dự phòng trên thiết bị hoặc hệ thống lưu trữ độc lập, định kỳ 01 tháng/lần.

3. Khi thực hiện nâng cấp, thay đổi cấu hình hệ thống phải thực hiện ngoài giờ làm việc.

4. Phải kiểm tra hoạt động tổng thể của hệ thống sau khi thay đổi cấu hình hoặc nâng cấp hệ thống.

5. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố:

a) Định kỳ hàng tháng hoặc khi có thay đổi, bộ phận chuyên trách thực hiện sao lưu, dự phòng hệ thống trên hệ thống độc lập như USB, DVD hoặc SAN.

b) Các dữ liệu sau yêu cầu sao lưu, dự phòng: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

6. Truy cập và quản lý cấu hình hệ thống:

a) Cấu hình hệ thống từ xa phải sử dụng các giao thức bảo mật có mã hóa thông tin như SSL, TSL, SSH, VPN.

b) Khi cấu hình hệ thống từ bên ngoài phải thông qua kết nối VPN.

c) Toàn bộ cấu hình hệ thống phải được lưu trên thiết bị hoặc hệ thống lưu trữ độc lập.

Điều 11. Quản lý an toàn máy chủ và ứng dụng

Quy định về quản lý an toàn máy chủ và ứng dụng:

1. Quy định với máy chủ

a) Hoạt động của máy chủ phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của ứng dụng.

b) Ảnh hệ điều hành phải được sao lưu dự phòng trên hệ thống lưu trữ độc lập định kỳ 01 tháng/lần.

c) Máy chủ phải được nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng.

d) Việc kết nối, gỡ bỏ máy chủ khỏi hệ thống phải được sự cho phép của Thủ trưởng đơn vị và xóa sạch dữ liệu.

đ) Có tài liệu liệt kê, cài đặt với những phần mềm hệ thống cài trong máy chủ.

2. Quy định với ứng dụng:

a) Hoạt động của ứng dụng phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của ứng dụng.

b) Ứng dụng phải được thiết lập chính sách xác thực; kiểm soát truy cập; có phương án bảo mật thông tin liên lạc và biện pháp bảo đảm an toàn ứng dụng và mã nguồn.

c) Ứng dụng phải được định kỳ kiểm tra đánh giá an toàn thông tin 2 năm/lần hoặc khi thay đổi, nâng cấp mở rộng.

3. Truy cập mạng của máy chủ:

a) Kết nối, truy cập máy chủ phải được kiểm soát bởi tường lửa hệ thống.

b) Đảm bảo các kết nối mạng trên máy chủ hoạt động liên tục, ổn định và an toàn.

4. Truy cập và quản trị máy chủ và ứng dụng:

a) Thay đổi mật khẩu mặc định sau khi được bàn giao tài khoản, mật khẩu.

b) Định kỳ 03 tháng thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng.

c) Chỉ cấp quyền quản lý máy chủ và ứng dụng cho cán bộ quản trị theo chức năng nhiệm vụ được giao.

d) Truy cập quản trị máy chủ và ứng dụng phải qua giao thức mã hóa như SSL, TLS, SSH và VPN.

e) Truy cập quản trị máy chủ và ứng dụng từ bên ngoài mạng phải qua kênh kết nối VPN.

5. Quy định về cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố:

a) Định kỳ hàng tháng hoặc khi nâng cấp ứng dụng phải sao lưu, dự phòng mã nguồn ứng dụng và cơ sở dữ liệu trên thiết bị hoặc hệ thống độc lập.

b) Dữ liệu lưu trữ phải được mã hóa cùng mã kiểm tra tính nguyên vẹn.

c) Dữ liệu lưu trữ phải được quản lý theo phiên bản và có quản lý truy cập.

Điều 12. Quản lý an toàn dữ liệu

1. Định kỳ hàng tháng hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

2. Bản sao lưu được lưu trữ trên thiết bị hoặc hệ thống độc lập.

Điều 13. Quản lý sự cố an toàn thông tin

1. Thực hiện cô lập hệ thống, ngắt kết nối với các hệ thống liên quan khác.

2. Khi có sự cố an toàn thông tin xảy ra, bộ phận chuyên trách phải sao lưu, dự phòng toàn bộ hiện trạng hệ thống trước khi xử lý sự cố.

3. Liên hệ với đầu mối ứng cứu sự cố theo thông tin được quy định tại khoản 2 Điều 5 Quy chế này.

Điều 14. Quản lý an toàn người sử dụng đầu cuối

1. Thông tin về thiết bị đầu cuối (tên, chủng loại, địa chỉ MAC, địa chỉ IP) phải được quản lý và cập nhật.

2. Các thiết bị đầu cuối phải được quản lý khi kết nối vào hệ thống mạng theo địa chỉ MAC, IP.

3. Khi truy cập và sử dụng thiết bị đầu cuối từ xa phải có cơ chế xác thực và sử dụng giao thức mạng an toàn.

4. Việc cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống phải được

cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt.

5. Máy chủ, máy tính cá nhân, hệ thống lưu trữ, thiết bị mạng, thiết bị bảo mật, các ứng dụng của đơn vị vận hành Hệ thống cơ sở dữ liệu truy xuất nguồn gốc nông lâm thủy sản thực phẩm tỉnh Hà Nam phải được bảo vệ bởi mật khẩu an toàn, có độ phức tạp cao, không sử dụng mật khẩu ngắn, mật khẩu mặc định.

6. Tất cả các máy tính tham gia vận hành Hệ thống cơ sở dữ liệu truy xuất nguồn gốc nông lâm thủy sản thực phẩm tỉnh Hà Nam phải được cài đặt bảo vệ bởi phần mềm phòng chống virus, phần mềm độc hại.

7. Đối với tài khoản người dùng sử dụng để đăng nhập vào hệ thống thông tin cơ sở dữ liệu truy xuất nguồn gốc nông lâm thủy sản thực phẩm tỉnh Hà Nam phải thiết lập mật khẩu có mức độ bảo mật cao, không sử dụng mật khẩu ngắn, mặc định nhằm đảm bảo an toàn, bảo mật thông tin của người dùng.

8. Tổ chức quản lý tài khoản, định danh người dùng trong hệ thống cơ sở dữ liệu truy xuất nguồn gốc nông lâm thủy sản thực phẩm tỉnh Hà Nam bao gồm: tạo mới, kích hoạt, sửa đổi và loại bỏ tài khoản; đối với người sử dụng tham gia vào vận hành hệ thống nghỉ việc hoặc chuyển công tác phải có biện pháp khóa tài khoản, hủy quyền truy cập, thu hồi các thiết bị liên quan tới hệ thống

Điều 15. Quản lý rủi ro an toàn thông tin mạng

Hồ sơ Quản lý rủi ro an toàn thông tin bao gồm các nội dung sau:

1. Danh mục tài sản thông tin, dữ liệu có trong hệ thống.

2. Đánh giá các rủi ro an toàn thông tin đối với mỗi loại tài sản.

3. Có phương án dự phòng và khôi phục sau sự cố đối với thông tin, dữ liệu và ứng dụng.

Điều 16. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

Quy định, quy trình về kết thúc vận hành, khai thác, thanh lý, hủy bỏ bao gồm các nội dung sau:

1. Khi kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống phải được bộ phận chuyên trách an toàn thông tin thực hiện kiểm tra, đánh giá bảo đảm an toàn thông tin.

2. Quá trình xử lý thông tin trên hệ thống phải được thực hiện khi thay đổi mục đích sử dụng hoặc gỡ bỏ theo phương án kỹ thuật được lãnh đạo Chi cục Chất lượng, Chế biến và Phát triển thị trường phê duyệt.

Chương IV
TỔ CHỨC BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 17. Trách nhiệm của Chi cục Chất lượng, Chế biến và Phát triển thị trường.

- Thực hiện trách nhiệm theo quy định tại Điều 22 Nghị định 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về về bảo đảm an toàn hệ thống thông tin theo cấp độ.

- Chủ trì tổ chức theo dõi, đôn đốc, kiểm tra, đánh giá việc thực hiện Quy chế này.

- Giao Phòng Nghiệp vụ là đầu mối, có trách nhiệm đề xuất sử dụng, phân công người theo dõi, sử dụng đảm bảo an toàn thông tin cho Hệ thống. Tuân thủ các quy định về an toàn thông tin được giao tại Quy chế này.

- Xây dựng hồ sơ đề xuất cấp độ an toàn thông tin và bảo đảm an toàn cho các hệ thống thông tin theo quy định của Luật An toàn thông tin mạng và các văn bản hướng dẫn thi hành Luật An toàn thông tin mạng.

- Tổ chức phổ biến, triển khai thực hiện các quy định bảo đảm an toàn thông tin mạng theo Quy chế này.

Điều 18. Trách nhiệm của cơ sở sản xuất kinh doanh

1. Nghiêm túc chấp hành các quy chế và các quy định khác của pháp luật về an toàn thông tin mạng.

2. Sử dụng, bảo mật tài khoản được cung cấp theo đúng mục đích, tuân thủ các quy định của pháp luật và Quy chế này.

3. Kịp thời phản ánh các lỗi phát sinh hoặc sự cố kỹ thuật, vướng mắc phát sinh trong quá trình khai thác thông tin trên hệ thống về cơ quan quản lý có thẩm quyền tại khoản 5 Điều 5 Quy chế này.

3. Chịu trách nhiệm trước pháp luật về các thông tin đã đăng tải.

Điều 19. Trách nhiệm của người tiêu dùng

Thực hiện nghiêm túc các quy định về quản lý, vận hành hệ thống tại đơn vị theo đúng các quy định hiện hành. Chấp hành đúng các quy định về an toàn thông tin tại Điều 14 Quy chế này.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 20. Xây dựng và công bố

1. Quy chế này được thông qua và công bố công khai trước khi áp dụng.

2. Tổ chức tuyên truyền, phổ biến cho các cơ quan, đơn vị, cơ sở sản xuất kinh doanh tham gia quản lý, sử dụng hệ thống để triển khai thực hiện.

Điều 21. Rà soát, cập nhật, bổ sung Quy chế

1. Định kỳ 03 năm hoặc khi có thay đổi Quy chế bảo đảm an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung.

2. Có hồ sơ lưu lại thông tin phản hồi của đối tượng áp dụng Quy chế trong quá trình triển khai, áp dụng Quy chế an toàn thông tin.