

QUYẾT ĐỊNH

**Ban hành Quy chế bảo đảm an toàn, an ninh cho
Hệ thống thông tin Trang thông tin điện tử và mạng nội bộ (Lan)
của Sở Nông nghiệp và PTNT tỉnh Đắk Nông**

GIÁM ĐỐC SỞ NÔNG NGHIỆP VÀ PTNT TỈNH ĐẮK NÔNG

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

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

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 và Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông về 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;

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 Quyết định số 10/2019/QĐ-UBND ngày 22/3/2019 của UBND tỉnh Đắk Nông ban hành Quy chế quản lý, vận hành, sử dụng và bảo đảm an toàn thông tin mạng truyền số liệu chuyên dùng cấp II tỉnh Đắk Nông;

Căn cứ Quyết định số 35/2023/QĐ-UBND ngày 11/12/2023 của UBND tỉnh Đắk Nông ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Nông nghiệp và Phát triển nông thôn tỉnh Đắk Nông;

Theo đề nghị của Chánh Văn phòng Sở Nông nghiệp và PTNT.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn, an ninh cho Hệ thống thông tin Trang thông tin điện tử và mạng nội bộ (Lan) của Sở Nông nghiệp và PTNT tỉnh Đắk Nông.

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

Điều 3. Chánh Văn phòng Sở; Trưởng các phòng chuyên môn, đơn vị trực thuộc và các cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:

- Như Điều 3;
- UBND tỉnh (báo cáo);
- Sở Thông tin và Truyền thông;
- GD và các PGD Sở;
- Lưu: VT, VP.

**KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Lê Quang Dân

QUY CHẾ

Bảo đảm an toàn, an ninh mạng cho Hệ thống thông tin Trang thông tin điện tử và mạng nội bộ (Lan) của Sở Nông nghiệp và PTNT
(Ban hành kèm theo Quyết định số: /QĐ-SNN ngày /12/2023 của Sở Nông nghiệp và PTNT tỉnh Đắk Nông)

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 các chính sách quản lý và các biện pháp nhằm bảo đảm an toàn thông tin cho phần mềm Hệ thống Trang thông tin điện tử cấp độ 2 và hệ thống mạng nội bộ (Lan) cấp độ 2 của Sở Nông nghiệp và PTNT tỉnh Đắk Nông, bao gồm:

- Phạm vi quản lý về vật lý và logic của tổ chức.
- Các ứng dụng, dịch vụ hệ thống cung cấp.
- Nguồn nhân lực bảo đảm an toàn thông tin.

2. Đối tượng áp dụng

a) Các phòng chuyên môn và đơn vị trực thuộc Sở Nông nghiệp và PTNT tỉnh Đắk Nông trong việc quản lý, khai thác, sử dụng Hệ thống thông tin Trang thông tin điện tử cấp độ 2 và mạng nội bộ (Lan) cấp độ 2 của Sở Nông nghiệp và PTNT tỉnh Đắk Nông.

b) Cơ quan, tổ chức, cá nhân có kết nối, sử dụng Hệ thống thông tin Trang thông tin điện tử cấp độ 2 và mạng nội bộ (Lan) cấp độ 2 của Sở Nông nghiệp và PTNT tỉnh Đắk Nông.

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ quản lý, vận hành, duy trì, phát triển và bảo đảm an toàn thông tin mạng phục vụ hoạt động của Hệ thống Trang thông tin điện tử cấp độ 2 và hệ thống mạng nội bộ (Lan) cấp độ 2 của Sở Nông nghiệp và PTNT tỉnh Đắk Nông.

Điều 2. 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 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 các của hệ thống thông tin Sở Nông

ng nghiệp và PTNT.

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 (ATTT) là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục trong quá trình: thu thập, tạo lập, xử lý, truyền tải, lưu trữ và sử dụng thông tin, dữ liệu; thiết kế, thiết lập và vận hành, nâng cấp, hủy bỏ hệ thống thông tin.

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.

Điều 3. 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 4. 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.

Sở Nông nghiệp và PTNT tỉnh Đắk Nông giao Văn phòng Sở chủ trì là đầu mối liên hệ 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 Trang thông tin điện tử cấp độ 2 và hệ thống mạng nội bộ (Lan) cấp độ 2 của Sở Nông nghiệp và PTNT tỉnh Đắk Nông.

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 Đắk Nông

- Bộ phận liên hệ: Phòng Công nghệ thông tin

- Số điện thoại: 02613.509.509

- Email: cntt.sttt@daknong.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>

Điều 5. Bảo đảm nguồn nhân lực

1. Tuyển dụng

Công chức được tuyển dụng vào vị trí việc làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng.

2. Trong quá trình làm việc

a) Trách nhiệm bảo đảm an toàn thông tin của người sử dụng, công chức quản lý và vận hành hệ thống

- Đối với người sử dụng:

+ Người sử dụng có trách nhiệm đảm bảo ATTT đối với từng vị trí công việc.

+ Phải được thường xuyên tổ chức quán triệt các quy định về ATTT, nhằm nâng cao nhận thức về trách nhiệm đảm bảo ATTT.

+ Phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp thiết bị.

- Đối với công chức quản lý và vận hành hệ thống

+ Công chức quản lý và vận hành hệ thống phải thiết lập phương pháp hạn chế truy cập mạng không dây, giám sát và điều khiển truy cập không dây, tổ chức sử dụng chứng thực và mã hóa để bảo vệ truy cập không dây tới hệ thống thông tin.

+ Công chức quản lý và vận hành hệ thống phải tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin.

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) Công chức chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc,

phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức;

b) Bộ phận chuyên trách thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi công chức thôi việc.

Chương II

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

Điều 6. Thiết kế an toàn hệ thống thông tin

1. Bộ phận chuyên trách xây dựng 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. Bộ phận chuyên trách xây dựng 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. Bộ phận chuyên trách xây dựng 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. Bộ phận chuyên trách xây dựng 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. Bộ phận chuyên trách 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 Sở quyết định trước khi thực hiện thay đổi.

Điều 7. Phát triển phần mềm thuê khoán

1. Yêu cầu có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán.

2. Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm:

a) Các nhà phát triển cung cấp mã nguồn phần mềm cho bộ phận chuyên trách.

b) Bộ phận chuyên trách có trách nhiệm quản lý và lưu trữ mã nguồn an toàn.

Điều 8. 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 Sở 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 9. 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 10. 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.

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 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) Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng.

e) Các bản quyền phần mềm cần được thống kê, quản lý thời gian hạn phục vụ cho việc gia hạn.

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 02 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) Chỉ mở cổng quản trị hệ thống từ vùng mạng LAN hoặc vùng mạng quản trị (nếu có)

c) Truy cập quản trị máy chủ từ bên ngoài mạng phải qua kênh kết nối VPN;

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

a) Thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng.

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

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

d) 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 11. Quản lý an toàn dữ liệu

1. Quy định dự phòng và khôi phục dữ liệu:

a) Định kỳ hàng tuần phải sao lưu, dự phòng cơ sở dữ liệu và dữ liệu nghiệp vụ (nếu có) 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.

2. 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.

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

Điều 12. 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 đưa ra dưới đây:

a) Sở Thông tin và Truyền thông tỉnh Đắk Nông

- Bộ phận liên hệ: Phòng Công nghệ thông tin
- Số điện thoại: 02613.509.509
- Email: cntt.sttt@daknong.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>

Điều 13. Quản lý an toàn người sử dụng đầu cuối

1. Khi kết nối thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB,... phải quét virus trước khi đọc hoặc sao chép dữ liệu.
2. Không sử dụng các máy tính thuộc sở hữu cá hoặc những thiết bị lưu trữ di động cá nhân vào mạng quản trị hoặc nghiệp vụ. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu.
3. Thiết lập mạng công cộng cho các máy tính thuộc sở hữu cá nhân hoặc những thiết bị lưu trữ di động cá nhân và có quản lý truy cập vùng mạng này với các vùng mạng khác trong hệ thống.
4. Máy tính người sử dụng phải được thiết lập chế độ cập nhật bản vá tự động và phần mềm phòng chống mã độc.

Điều 14. Quản lý rủi ro an toàn thông tin mạng

Đơn vị vận hành xây dựng và ban hành 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 15. 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. Thiết bị công nghệ thông tin có chứa dữ liệu (máy tính, thiết bị lưu trữ,...) khi bị hỏng phải được công chức vận hành kiểm tra, sửa chữa, khắc phục. Phải có biện pháp kiểm tra, giám sát đảm bảo không để lọt lộ thông tin hay lây nhiễm mã độc đối với máy tính mang ra bên ngoài sửa chữa, bảo hành.

2. Trước khi tiến hành thanh lý/loại bỏ thiết bị công nghệ thông tin cũ, phải áp dụng các biện pháp kỹ thuật xóa bỏ hoàn toàn dữ liệu người dùng đã tạo ra, đảm bảo không thể phục hồi.

3. Các phương tiện và thiết bị công nghệ thông tin: Máy tính cá nhân (PC), máy tính xách tay, máy chủ, các thiết bị mạng, phương tiện lưu trữ như CD/DVD, thẻ nhớ, ổ cứng phải xóa sạch dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng.

Chương IV

TỔ CHỨC BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 16. Trách nhiệm của Sở Nông nghiệp và PTNT

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

Điều 17. Trách nhiệm của Văn phòng Sở Nông nghiệp và PTNT

1. Giao Văn phòng Sở là bộ phận chuyên trách về an toàn thông tin, có trách nhiệm bảo đảm an toàn thông tin cho các hệ thống thông tin.

2. Tuân thủ các quy định về trách nhiệm của bộ phận chuyên trách về an toàn thông tin được giao tại Quy chế này.

Điều 18. Trách nhiệm của người 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 19. Xây dựng và công bố

Quy chế này được tổ chức/bộ phận trình người đứng đầu đơn vị vận hành trước khi công bố áp dụng.

Điều 20. 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 chính sách trong quá trình triển khai, áp dụng chính sách an toàn thông tin.