UBND TỈNH HƯNG YÊN
SỞ NÔNG NGHIỆP VÀ PTNT

Số: 90/QĐ-SNN

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

Hưng Yên, ngày 30 tháng 3 năm 2016

QUYẾT ĐỊNH

Ban hành Quy chế đảm bảo an toàn, an ninh thông tin của Sở Nông nghiệp và Phát triển nông thôn tỉnh Hưng Yên

GIÁM ĐỐC SỞ NÔNG NGHIỆP VÀ PTNT

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

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ quy định về ứng dụng công nghệ thông tin trong hoạt động của cơ quan Nhà nước;

Căn cứ Thông tư số 23/2011/TT-BTTTT ngày 11/08/2011 của Bộ Thông tin và Truyền thông Quy định về việc quản lý, vận hành, sử dụng và bảo đảm an toàn thông tin trên Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;

Căn cứ Quyết định số 1159/QĐ-UBND ngày 10/6/2010 của UBND tỉnh Hưng Yên về chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức bộ máy của Sở Nông nghiệp và Phát triển nông thôn tỉnh Hưng Yên;

Căn cứ Quyết định 05/2016/QĐ-UBND ngày 17/3/2016 của UBND tỉnh Hưng Yên về việc ban hành Quy chế đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Hưng Yên;

Xét đề nghị của Chánh Văn phòng Sở,

QUYẾT ĐỊNH

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn, an ninh thông tin của Sở Nông nghiệp và Phát triển nông thôn tỉnh Hưng Yên.

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

Điều 3. Chánh Văn phòng sở, Trưởng các phòng, ban, đơn vị và các cá nhân liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Lãnh đạo sở;
- Như Điều 3;
- Lưu VT.

GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ NÔNG NGHIỆP VÀ PHÁT TRIỂN NÔNG THÔN
TỈNH HƯNG YÊN

Nguyễn Văn Doanh

UBND TỈNH HƯNG YÊN
SỞ NÔNG NGHIỆP VÀ PTNT

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

QUY CHẾ
Đảm bảo an toàn, an ninh thông tin của Sở Nông nghiệp và Phát triển nông thôn tỉnh Hưng Yên

(Ban hành kèm theo Quyết định số 90 /QĐ-SNN ngày 30/3/2016 của Sở NN và PTNT)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về công tác đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của các phòng, ban, đơn vị trực thuộc Sở Nông nghiệp và PTNT.

Điều 2. Đối tượng áp dụng

1. Quy chế này áp dụng đối với các phòng, ban, đơn vị trực thuộc Sở.

2. Cán bộ, công chức, viên chức (sau đây gọi tắt là người dùng) đang làm việc trong các phòng, ban, đơn vị nêu tại Khoản 1 điều này và các tổ chức, cá nhân có liên quan áp dụng Quy chế này trong việc đảm bảo an toàn thông tin tại các phòng, ban, đơn vị.

Điều 3. Giải thích từ ngữ

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

1. Hệ thống thông tin là tập hợp thiết bị 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 số.

2. An toàn thông tin là sự bảo vệ thông tin và các hệ thống thông tin 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.

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

4. Thông tin số là thông tin được tạo lập bằng phương pháp dùng tín hiệu số.

5. 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 4. Mục đích, nguyên tắc đảm bảo an toàn thông tin

1. Tăng cường khả năng phòng chống nguy cơ tấn công, xâm nhập hệ thống thông tin và ngăn chặn, khắc phục kịp thời các sự cố gây mất an toàn thông tin trên môi trường mạng.

2. Công tác đảm bảo an toàn, bảo mật thông tin trên môi trường mạng là yêu cầu bắt buộc trong quá trình thiết kế, vận hành, nâng cấp hệ thống thông tin của cơ quan nhà nước.

3. Thông tin số được quy định danh mục bí mật nhà nước, văn bản điện tử có nội dung mật không được truyền đưa trên môi trường mạng và phải được phân loại, lưu trữ, bảo vệ theo quy định của pháp luật về bảo vệ bí mật nhà nước. Trường hợp đặc biệt, cần truyền thông tin mật trên mạng, phải được Thủ trưởng cơ quan, đơn vị cho phép; trước khi truyền thông tin phải được mã hóa theo quy định của Luật Cơ yếu.

Điều 5. Các hành vi bị nghiêm cấm

1. Ngăn chặn trái pháp luật việc truyền tải thông tin trên mạng; can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sửa chữa, sao chép, làm sai lệch trái phép thông tin trên mạng.

2. Cản trở trái pháp luật hoạt động các hệ thống thông tin của tỉnh; phá hoại cơ sở hạ tầng thông tin, phá hoại thông tin trên môi trường mạng; gây ảnh hưởng tới khả năng truy nhập hợp pháp của người sử dụng tới hệ thống thông tin.

3. Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin cho hệ thống thông tin; tạo, cài đặt, phát tán phần mềm độc hại, vi rút máy tính, thư rác; xâm nhập trái phép, chiếm quyền điều khiển hệ thống thông tin.

4. Lợi dụng mạng để tuyên truyền, chống phá Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; thực hiện các hành vi gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội; phá hại khối đại đoàn kết toàn dân; quảng cáo, tuyên truyền, mua bán hàng hóa, dịch vụ bị cấm; truyền bá tác phẩm báo chí, văn học, nghệ thuật, xuất bản phẩm bị cấm.

5. Tiết lộ bí mật nhà nước, bí mật quân sự, an ninh, kinh tế, đối ngoại và những bí mật khác do pháp luật quy định.

6. Các hành vi bị nghiêm cấm khác theo quy định của pháp luật.

Chương II

NỘI DUNG ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 6. Về quản lý cán bộ, công chức, viên chức và người lao động

1. Các phòng, ban, đơn vị phải xây dựng các yêu cầu, trách nhiệm đảm bảo an toàn thông tin đối với từng công việc. Trước khi tiếp nhận nhân sự, các phòng, ban, đơn vị phải kiểm tra khả năng đáp ứng các yêu cầu về an toàn thông

tin nhân sự mới; trong các hợp đồng lao động, phải có các điều khoản về trách nhiệm đảm bảo an toàn thông tin nội bộ cơ quan.

2. Các phòng, ban đơn vị phải thường xuyên tổ chức quán triệt các quy định về an toàn thông tin, nhằm nâng cao nhận thức về trách nhiệm đảm bảo an toàn thông tin của từng cá nhân trong cơ quan.

3. Hủy tài khoản, quyền truy cập các hệ thống thông tin, thu hồi lại các tài sản liên quan đến hệ thống thông tin (thư mục lưu trữ, thư điện tử, máy vi tính, ...) đối với các cá nhân nghỉ việc, chuyển công tác.

Điều 7. Quản lý mạng nội bộ

Hệ thống mạng nội bộ (LAN) của Sở được thiết lập và quản lý theo quy trình. Các thiết bị Router, Switch được đặt cố định, nguồn điện cung cấp cho hệ thống này phải ổn định, có điều hòa nhiệt độ để bảo đảm về nhiệt độ và độ ẩm phù hợp với yêu cầu tiêu chuẩn kỹ thuật phòng máy, có biện pháp bảo vệ ngăn chặn xâm nhập trái phép vào phòng chứa các thiết bị này.

Điều 8. Quản lý thiết trang thiết bị và hạ tầng công nghệ thông tin

1. Thiết bị chuyển mạch (Switch):

Thiết bị chuyển mạch mạng tin học của Sở phải bảo đảm khả năng cung cấp các chức năng quản trị nhằm tăng cường độ an toàn và bảo mật cho hệ thống mạng như: cung cấp khả năng từ chối các kết nối không mong muốn hay trái phép vào hệ thống trên từng cổng, quy định địa chỉ IP cho từng cổng và khống chế số lượng kết nối vào hệ thống mạng nội bộ thông qua thiết bị chuyển mạch.

2. Máy tính, thiết bị tháo lắp (USB, máy tính sách tay):

a) Người dùng có trách nhiệm quản lý, bảo quản thiết bị được giao sử dụng; không tự ý thay đổi cấu hình hoặc tháo lắp, sửa chữa các thiết bị trên máy tính; phải đặt mật khẩu truy cập vào máy tính của mình và định kỳ ít nhất 3 tháng một lần đổi mật khẩu cho máy tính; cài đặt cơ chế tự động thoát cho máy tính khi không sử dụng; không tự ý liên hệ và cho người ngoài cơ quan sử dụng, sửa chữa máy tính hoặc cắm các thiết bị bên ngoài vào máy tính.

b) Các thiết bị gắn ngoài như: USB, thẻ nhớ, máy tính xách tay, máy tính bảng, ... của cơ quan trang bị hoặc tự có, khi cắm vào máy tính hoặc mạng LAN, internet, wifi của cơ quan phải kiểm tra, đảm bảo không có virus hoặc các phần mềm độc hại khác.

Điều 9. Đảm bảo an toàn dữ liệu

1. Đối với các phần mềm:

a. Các phần mềm có bản quyền đã được cơ quan, đơn vị mua hoặc được cung cấp như: Phần mềm kế toán, phần mềm Quản lý văn bản và điều hành công việc, hệ thống thư điện tử công vụ, ... phải được đảm bảo hoạt động liên tục, đảm bảo tính chính xác của thông tin, không gây ra sự cố mất dữ liệu.

b) Cán bộ, công chức, viên chức quản lý, sử dụng, bảo mật các tài khoản để đăng nhập vào các phần mềm. Ít nhất trong vòng 03 tháng phải thay đổi mật khẩu sử dụng.

c) Khi kết thúc làm việc với các phần mềm, nhất thiết phải thực hiện thao tác thoát khỏi ứng dụng trước khi rời khỏi máy tính, nhằm hạn chế các nguy cơ xâm nhập trái phép gây mất an toàn, an ninh thông tin.

2. Truyền tải, lưu trữ, sao chép thông tin:

a) Người sử dụng có trách nhiệm tự quản lý dữ liệu trên máy tính phục vụ công tác chuyên môn của mình, định kỳ ít nhất 03 tháng một lần, phối hợp với chuyên viên chuyên trách CNTT tiến hành sao lưu, sao chép dữ liệu trong máy tính ra bộ nhớ ngoài (ổ cứng bên ngoài máy tính, đĩa CD, USB, thiết bị sao lưu dữ liệu NAT), các thiết bị lưu trữ thông tin này phải được bảo quản ở nơi an toàn và bảo mật.

b) Không được lưu trữ dữ liệu và sao chép thông tin trên phân vùng đĩa cứng cài đặt hệ điều hành (ổ cứng C), việc lưu trữ dữ liệu và sao chép thông tin chỉ thực hiện trên đĩa cứng D, E giúp cho việc phục hồi dữ liệu được dễ dàng khi có sự cố máy tính.

c) Hạn chế việc chia sẻ thông tin, dữ liệu trên máy tính thông qua tính năng share full của hệ điều hành Windows.

3. Chống mã độc, virus:

a) Toàn bộ máy tính của cơ quan đều phải cài đặt phần mềm diệt virus có bản quyền để bảo đảm an toàn, an ninh thông tin để phát hiện, loại trừ những đoạn mã độc (virus, trojan, worm …) được truyền tải bởi: thư điện tử, tập tin đính kèm từ internet, thiết bị lưu trữ tháo lắp nhằm khai thác lỗ hổng của hệ thống thông tin; thường xuyên cập nhật các phiên bản mới, các bản vá lỗi của các phần mềm hệ thống (đối với phần mềm có bản quyền), phần mềm diệt virus, phần mềm ứng dụng, … để đảm bảo chương trình quét virus luôn được cập nhật mới nhất.

b) Người dùng không được truy cập thông tin hoặc nhấp chuột vào trang web có đường dẫn lạ không rõ về nội dung hoặc các trang web độc hại; không tải và cài đặt các phần mềm không rõ nguồn gốc; hạn chế tải các file có dung lượng lớn và không xem các video clip trong giờ làm việc ảnh hưởng đến tốc độ đường truyền của hệ thống. Các tập tin gửi đính kèm bởi thư điện tử hoặc tải xuống từ internet hay các thiết bị lưu gắn vào hệ thống cần được kiểm tra để phòng chống lây nhiễm virus hoặc phần mềm gián điệp gây mất thông tin.

Điều 10. Đảm bảo an toàn cho Trang thông tin điện tử của Sở

Thường xuyên phối hợp với Trung tâm tin học UBND tỉnh, Sở Thông tin và Truyền thông thực hiện việc thay đổi mật khẩu với độ mạnh cao, sao lưu, phục hồi toàn bộ nội dung trang web để đảm bảo khi có sự cố có thể khắc phục lại trong 24 giờ.

Điều 11. Giải quyết và khắc phục sự cố về an toàn, an ninh thông tin

1. Trách nhiệm của người sử dụng:

Thông tin, báo cáo kịp thời cho cán bộ chuyên trách CNTT và Lãnh đạo phòng, ban, đơn vị khi phát hiện các sự cố gây mất an toàn, an ninh thông tin trong quá trình tham gia vào hệ thống thông tin của cơ quan, đơn vị; tích cực phối hợp với cán bộ chuyên trách CNTT và các cơ quan liên quan trong quá trình khắc phục sự cố.

2. Trách nhiệm của cán bộ chuyên trách CNTT:

Khi phát hiện hoặc tiếp nhận sự cố gây mất an toàn, an ninh thông tin, cán bộ chuyên trách CNTT phải thực hiện giải quyết theo đúng quy trình xử lý sự cố; trong trường hợp sự cố xảy ra ngoài khả năng giải quyết của cơ quan, phải báo cáo khẩn cấp bằng điện thoại tới bộ phận phụ trách CNTT của Sở Thông tin và Truyền thông để được hỗ trợ, hướng dẫn và phối hợp khắc phục sự cố; đồng thời tham mưu văn bản báo cáo sự cố gửi Sở Thông tin và Truyền thông, Công an tỉnh theo quy định.

Chương III

TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 12. Trách nhiệm của Văn phòng sở

1. Giúp Giám đốc Sở chỉ đạo, hướng dẫn, theo dõi, đôn đốc, kiểm tra các phòng, ban, đơn vị trong công tác đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng CNTT.

2. Phân công cán bộ chuyên trách CNTT, đảm bảo an toàn, an ninh thông tin trước khi tiến hành các hoạt động quản lý, vận hành hệ thống thông tin.

3. Phân bổ kinh phí để trang bị các thiết bị phần cứng, phần mềm liên quan đến công tác đảm bảo an toàn thông tin, đầu tư thiết bị tường lửa, các chương trình chống Spam, Virus có bản quyền trên máy vi tính của cán bộ công chức, viên chức trong Sở.

4. Quan tâm đào tạo, bồi dưỡng nguồn nhân lực có kiến thức, trình độ về CNTT; trang bị đầy đủ kiến thức bảo mật cơ bản cho cán bộ, công chức, viên chức trước khi truy nhập và sử dụng hệ thống thông tin.

5. Khi có sự cố hoặc nguy cơ mất an toàn, an ninh thông tin, kịp thời cử cán bộ phối hợp chặt chẽ với cơ quan chuyên môn trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn, an ninh thông tin; tạo điều kiện thuận lợi cho cơ quan chức năng tham gia khắc phục sự cố và thực hiện đúng theo hướng dẫn.

Điều 13. Trách nhiệm của cán bộ, công chức, viên chức các phòng, ban, đơn vị.

1. Chấp hành nghiêm các quy định, quy trình nội bộ, Quy chế này và các quy định khác của pháp luật về an toàn thông tin; chịu trách nhiệm đảm bảo an toàn thông tin trong phạm vi trách nhiệm và quyền hạn được giao;

2. Mỗi cán bộ, công chức, viên chức có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp các thiết bị trên máy tính; không được vào các trang web không rõ về nội dung; không tải và cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn; không nhấp chuột vào các đường dẫn lạ không rõ về nội dung.

3. Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin, phải báo cáo ngay với cấp trên và bộ phận chuyên trách công nghệ thông tin của đơn vị để kịp thời ngăn chặn và xử lý.

Điều 14. Trách nhiệm của các phòng, ban, đơn vị

1. Lãnh đạo các phòng, ban, đơn vị có trách nhiệm tổ chức thực hiện quy định này và chịu trách nhiệm trước Giám đốc sở trong công tác đảm bảo an toàn thông tin của đơn vị.

2. Phân công một bộ phận hoặc cán bộ phụ trách an toàn thông tin của đơn vị; tạo điều kiện để các cán bộ phụ trách an toàn thông tin được học tập, nâng cao trình độ về an toàn thông tin.

3. Xây dựng quy định, quy trình nội bộ về đảm bảo an toàn thông tin phù hợp với Quy chế này và các quy định của pháp luật.

4. Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố xảy ra một cách kịp thời, nhanh chóng và đạt hiệu quả.

5. Phối hợp chặt chẽ với Sở Thông tin và Truyền thông và Công an tỉnh trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn, an ninh thông tin.

6. Định kỳ hàng quý, các phòng, ban, đơn vị lập báo cáo về tình hình an toàn thông tin và gửi về Sở.

Điều 15. Trách nhiệm của công chức chuyên trách CNTT

Công chức chuyên trách CNTT có trách nhiệm giúp Giám đốc Sở, Chánh Văn phòng Sở:

1. Trực tiếp thiết lập các biện pháp kỹ thuật bảo đảm an toàn cho các máy tính cá nhân trong cơ quan, đơn vị mình; hướng dẫn người sử dụng tuân thủ các biện pháp đảm bảo an toàn, an ninh thông tin trong khai thác, sử dụng phần mềm và các trang thiết bị CNTT.

2. Thực hiện cấp, thu hồi, quản lý tất cả các tài khoản truy cập vào hệ thống thông tin của Sở.

2. Thực hiện cấp, thu hồi, quản lý tất cả các tài khoản truy cập vào hệ thống thông tin của Sở.

3. Chịu trách nhiệm xây dựng, triển khai các biện pháp quản lý vận hành, quản lý kỹ thuật, xây dựng phương án hạn chế, khắc phục rủi ro và nguy cơ có thể xảy ra.

4. Kịp thời khắc phục sự cố về CNTT; trong trường hợp sự cố xảy ra ngoài khả năng giải quyết, kịp thời báo cáo với Lãnh đạo Sở, đồng thời phối hợp với cơ quan chuyên môn để khắc phục.

5. Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm tra, phát hiện và khắc phục các sự cố mất an toàn, an ninh thông tin tại cơ quan, đơn vị mình.

6. Định kỳ báo cáo tình hình an toàn, an ninh của hệ thống CNTT của Sở cho các cơ quan liên quan theo quy định.

Chương IV

TỔ CHỨC THỰC HIỆN

Điều 16. Khen thưởng và xử lý vi phạm

1. Thực hiện tốt Quy chế đảm bảo an toàn, an ninh thông tin của Sở là một trong những điều kiện để xem xét khen thưởng cuối năm theo quy định.

2. Các cơ quan, đơn vị, cá nhân có hành vi vi phạm Quy chế này tùy theo tính chất, mức độ vi phạm sẽ bị xử lý theo quy định của pháp luật.

Điều 17. Tổ chức thực hiện

Văn phòng Sở chủ trì, phối hợp với thủ trưởng các phòng, ban, đơn vị trực thuộc hướng dẫn, đôn đốc và kiểm tra việc thực hiện Quy chế đến toàn bộ cán bộ, công chức, viên chức của Sở; hàng năm đánh giá tổng kết, báo cáo Lãnh đạo Sở.

Điều 18. Điều khoản thi hành

Trong quá trình thực hiện Quy chế này, nếu có vấn đề phát sinh hoặc khó khăn, cần phản ánh kịp thời về Văn phòng Sở để tổng hợp, báo cáo Lãnh đạo Sở xem xét sửa đổi, bổ sung cho phù hợp./.

GIÁM ĐỐC



Nguyễn Văn Doanh