UBND TỈNH NINH BÌNH
SỞ NÔNG NGHIỆP VÀ PTNT

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

Số: 329/QĐ-SNN

Ninh Bình, ngày 06 tháng 7 năm 2018

QUYẾT ĐỊNH

Ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin tại Sở Nông nghiệp và PTNT tỉnh Ninh Bình

GIÁM ĐỐC SỞ NÔNG NGHIỆP VÀ PTNT TỈNH NINH BÌNH

Căn cứ Quyết định số 37/2015/QĐ-UBND, ngày 28/12/2015 của UBND tỉnh Ninh Bình về việc ban hành quy định chức năng, nhiệm vụ, quyền hạn, cơ cấu tổ chức của Sở Nông nghiệp & PTNT tỉnh Ninh Bình;

Căn cứ Quyết định số 238/QĐ-UBND, ngày 22/4/2016 của UBND tỉnh Ninh Bình về việc phê duyệt cơ cấu tổ chức các đơn vị trực thuộc Sở Nông nghiệp & PTNT tỉnh Ninh Bình;

Căn cứ Quyết định số 15/2016/QĐ-UBND, ngày 06/7/2016 của UBND tỉnh Ninh Bình 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 thuộc phạm vi quản lý của tỉnh Ninh Bình;

Theo 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 trong hoạt động ứng dụng công nghệ thông tin tại Sở Nông nghiệp và PTNT tỉnh Ninh Bình.

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

Điều 3. Chánh Văn phòng Sở; Thủ trưởng các đơn vị trực thuộc Sở chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như điều 3;
- Sở Thông tin và Truyền thông Ninh Bình;
- Lãnh đạo Sở;
- Trang TTĐT Sở;
- Lưu: VT-MC.

GIÁM ĐỐC

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

Vũ Nam Tiến

UBND TỈNH NINH BÌNH
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 trong hoạt động ứng dụng công nghệ thông tin tại Sở Nông nghiệp và PTNT tỉnh Ninh Bình

(Ban hành kèm theo Quyết định số 329 /QĐ-SNN ngày 06 / 7 /2018 của Sở Nông nghiệp và PTNT tỉnh Ninh Bình)

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 trong hoạt động ứng dụng công nghệ thông tin (CNTT) của Sở Nông nghiệp và PTNT.

Điều 2. Đối tượng áp dụng

Quy chế này áp dụng cho tất cả các đơn vị trực thuộc Sở; các cán bộ, công chức, viên chức (CBCCVC) tham gia vận hành, khai thác và ứng dụng CNTT trong quá trình xử lý công việc.

Điều 3. Giải thích từ ngữ

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

1. *An toàn thông tin* là bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin đối với nguy cơ tự nhiên hoặc do con người gây ra. An toàn thông tin bao gồm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng.

2. *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.

3. *Hệ thống thông tin* là tập hợp các thiết bị viễn thông, CNTT, bao gồm phần cứng, phần mềm và cơ sở dữ liệu phục vụ cho hoạt động lưu trữ, xử lý, truyền đưa, chia sẻ, trao đổi, cung cấp và sử dụng thông tin.

4. *Mạng* là khái niệm chung dùng để chỉ mạng viễn thông cố định, di động, Internet và mạng máy tính.

5. *Hạ tầng kỹ thuật* là tập hợp thiết bị tính toán (máy chủ, máy trạm), thiết bị ngoại vi, thiết bị kết nối mạng, thiết bị phụ trợ, mạng nội bộ, mạng diện rộng.

6. *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.

7. *Phòng máy chủ* là nơi đặt tập trung các thiết bị CNTT dùng chung, như: máy chủ (server), các thiết bị mạng, an toàn mạng.... của cơ quan.

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

9. *Thông tin cá nhân* là thông tin gắn với việc xác định danh tính của một người cụ thể.

10. *Xử lý thông tin cá nhân* là việc thực hiện một hoặc một số thao tác thu thập, biên tập, sử dụng, lưu trữ, cung cấp, chia sẻ, phát tán thông tin cá nhân trên mạng nhằm mục đích thương mại.

11. *Máy tính cá nhân* là máy tính để bàn (Desktop Computer), máy tính xách tay (Laptop), máy tính bảng (Tablet Computer) và tương đương được CBCCVC sử dụng để thực hiện những nhiệm vụ theo chuyên môn được giao.

12. *Máy trạm* là máy tính cá nhân khi được kết nối với hệ thống mạng nội bộ của cơ quan, đơn vị.

13. *Bản vá lỗ hổng bảo mật* của một phần mềm là công cụ được tạo ra để sửa một hoặc một số lỗi cụ thể đã gây ra nguy cơ mất an toàn, an ninh thông tin khi sử dụng phần mềm.

14. *Sản phẩm an toàn thông tin mạng* là phần cứng, phần mềm có chức năng bảo vệ thông tin, hệ thống thông tin.

15. *Dịch vụ an toàn thông tin mạng* là dịch vụ bảo vệ thông tin, hệ thống thông tin.

Điều 4. Nguyên tắc bảo đảm an toàn, an ninh thông tin

1. Việc bảo đảm an toàn, an ninh thông tin là yêu cầu bắt buộc trong quá trình thiết kế, xây dựng, vận hành, nâng cấp và hủy bỏ hạ tầng kỹ thuật, hệ thống thông tin của cơ quan, đơn vị.

2. Hạ tầng kỹ thuật, hệ thống thông tin phải được định kỳ kiểm tra, đánh giá hoặc kiểm định về mặt an toàn, an ninh thông tin phù hợp với các tiêu chuẩn, quy chuẩn kỹ thuật quy định.

3. Thông tin số thuộc quy định danh mục bí mật nhà nước của các cơ quan, đơn vị phải được phân loại, lưu trữ, bảo vệ trên cơ sở quy định của pháp luật về bảo vệ bí mật nhà nước.

Điều 5. Các hành vi bị nghiêm cấm

1. Ngăn chặn, cản trở trái phép việc truy cập, truyền tải thông tin của cơ quan, cá nhân, gây nguy hại, xóa, làm sai lệch thông tin trên mạng; ảnh hưởng tới hoạt động bình thường của hệ thống thông tin, khả năng truy cập hợp pháp của người sử dụng tới hệ thống thông tin trừ trường hợp pháp luật cho phép.

2. Tấn công, vô hiệu hóa trái phép làm mất tác dụng của các biện pháp bảo vệ an toàn, an ninh thông tin; tấn công, chiếm quyền điều khiển, thu thập thông tin trái phép đối với hệ thống thông tin.

3. Tạo, cài đặt, phát tán thư rác, tin nhắn rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.

4. Lợi dụng mạng truyền bá tư tưởng, văn hóa độc hại, đồi trụy, kích động, chống phá các chủ trương đường lối của Đảng, chính sách pháp luật của Nhà nước.

Chương II
NỘI DUNG ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 6. Đảm bảo an toàn mạng và hạ tầng kỹ thuật

1. Phòng máy chủ

a) Được bố trí độc lập; cán bộ phụ trách CNTT trực tiếp quản lý; áp dụng các biện pháp và kiểm soát ra vào thích hợp;

b) Phòng máy chủ phải đảm bảo các điều kiện như: được bố trí ở khu vực có điều kiện an ninh tốt; khô ráo, có điều hòa không khí; nguồn cung cấp điện ổn định và có dự phòng; có bình chữa cháy hoặc hệ thống tự động cảnh báo, chữa cháy khẩn cấp; phòng, chống sét;

2. Thiết lập các cơ chế bảo vệ mạng nội bộ:

a) Hệ thống mạng không dây (Wifi) phải được thiết lập mật khẩu truy cập đủ mạng và phân lớp mạng riêng cho các máy tính truy cập mạng không dây, định kỳ thay đổi mật khẩu, chậm nhất ba tháng phải đổi một lần;

b) Xây dựng và áp dụng các biện pháp bảo vệ, giám sát, ghi nhật ký hoạt động và quản lý hạ tầng kỹ thuật, hệ thống thông tin nhằm phòng ngừa, ngăn chặn và phát hiện sớm các truy cập trái phép;

c) Kiểm soát chặt chẽ việc cài đặt các phần mềm lên máy chủ và máy trạm, đảm bảo tuân thủ quy định quản lý an toàn, an ninh thông tin của cơ quan, đơn vị và các quy định khác có liên quan;

d) Theo dõi thường xuyên tình trạng lây nhiễm và thực hiện loại bỏ phần mềm độc hại khỏi hệ thống thông tin.

3. An toàn cho máy tính cá nhân:

a) Kích hoạt và thiết lập chế độ tự động cập nhật bản vá lỗ hổng bảo mật cho các phần mềm trên mỗi máy tính cá nhân; đặt mật khẩu đăng nhập, chế độ bảo vệ màn hình cho máy tính cá nhân nhằm hạn chế các nguy cơ xâm nhập trái phép;

b) Cài đặt phần mềm phòng, chống virus, mã độc cho tất cả các máy tính trong mạng nội bộ của phòng, ban, đơn vị, thiết lập chế độ cập nhật hàng ngày cho phần mềm này;

c) Không cài đặt phần mềm không rõ nguồn gốc, xuất xứ; không truy cập những trang web có nội dung không lành mạnh, không mở những thư điện tử không rõ địa chỉ người gửi…;

d) Hạn chế sử dụng chức năng chia sẻ thư mục (Sharing). Khi sử dụng chức năng này thiết lập cơ chế chỉ đọc (Read Only) đối với những thư mục được chia sẻ trong mạng nội bộ. Chỉ sử dụng cơ chế cho phép toàn quyền đọc, ghi (Read, Write) khi thật cần thiết yêu cầu phải sử dụng mật khẩu khi truy cập thư mục chia sẻ và thực hiện thu hồi chức năng này sau khi đã sử dụng xong.

4. An toàn cho máy chủ:

a) Thiết lập chế độ tự động cập nhật bản vá lỗ hổng bảo mật cho phần mềm hệ điều hành và các phần mềm ứng dụng được cài đặt trên máy chủ; đóng tất cả các cổng (Port) dịch vụ khi không sử dụng; thiết lập chính sách ghi lưu tập trong quá trình hoạt động (Log file) của mỗi máy chủ theo định kỳ từ 3 tháng trở lên;

b) Khi cần kết nối từ xa, nhất là từ Internet vào máy chủ để quản trị, phải sử dụng phương thức kết nối có mã hóa (ví dụ: SSH, VPN...);

c) Các máy chủ chỉ dùng để cài đặt các phần mềm, dịch vụ dùng chung của cơ quan, đơn vị; không cài đặt các phần mềm không rõ nguồn gốc, phần mềm không có nhu cầu sử dụng. Không sử dụng máy chủ để duyệt web đọc báo, xem tin tức, chơi điện tử....;

d) Cài đặt phần mềm phòng, chống virus, mã độc cho máy chủ, đồng thời đảm bảo các phần mềm phòng, chống virus, mã độc này luôn được cập nhật khả năng nhận dạng virus, mã độc mới từ nhà sản xuất.

5. An toàn khi sử dụng các thiết bị lưu trữ ngoài:

a) Việc sử dụng các 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;

b) Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu.

Điều 7. An toàn dữ liệu, cơ sở dữ liệu và phần mềm ứng dụng CNTT

1. Quản lý chặt chẽ việc di chuyển các trang thiết bị CNTT lưu trữ dữ liệu, nhất là các thông tin thuộc danh mục bí mật Nhà nước.

2. Quản lý và phân quyền truy cập phần mềm và cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ của người sử dụng.

3. An toàn khi khai thác, sử dụng các phần mềm dùng chung của tỉnh:

a) Nghiêm cấm tiết lộ tài khoản đăng nhập, đấu nối, truy cập trái phép vào hệ thống các phần mềm dùng chung của tỉnh;

b) Tài khoản truy cập các phần mềm dùng chung của tỉnh phải đổi mật khẩu mặc định ngay sau khi được cấp, định kỳ hàng tháng thay đổi mật khẩu, đặt mật khẩu với độ an toàn cao; không đặt chế độ ghi nhớ mật khẩu khi sử dụng...;

c) Khi khai thác, sử dụng các phần mềm dùng chung của tỉnh tại các điểm truy cập Internet công cộng, tuyệt đối không đặt chế độ lưu trữ mật khẩu trong các trình duyệt.

Điều 8. Đảm bảo an toàn trong hoạt động trao đổi thông tin trên mạng

1. Việc gửi thông tin trên mạng phải đảm bảo:

a) Không giả mạo nguồn gốc của thông tin;

b) Tuân thủ quy định này và quy định của pháp luật có liên quan,

2. Khuyến khích áp dụng công nghệ mã hóa, chữ ký số... khi chia sẻ, lưu trữ, trao đổi thông tin trên môi trường mạng.

Điều 9. Bảo vệ bí mật Nhà nước trong công tác ứng dụng CNTT

1. Không được sử dụng máy tính nối mạng để soạn thảo văn bản, chuyển giao, lưu trữ thông tin có nội dung thuộc bí mật nhà nước; cung cấp tin, tài liệu và đưa thông tin bí mật nhà nước trên mạng.

2. Không được in, sao chụp tài liệu bí mật nhà nước trên xác thiết bị kết nối mạng.

3. Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật, các cơ quan phải báo cáo và có sự giám sát, quản lý chặt chẽ của cơ quan có thẩm quyền.

4. Có biện pháp quản lý chặt chẽ trong việc sử dụng và thanh lý tài sản khác trang thiết bị CNTT lưu trữ các thông tin thuộc danh mục bí mật nhà nước. Tuân thủ Pháp lệnh bảo vệ bí mật Nhà nước và các quy định khác có liên quan của Nhà nước về công tác bảo vệ bí mật nhà nước.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 10. Trách nhiệm của Văn phòng Sở

1. 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 các rủi ro và nguy cơ có thể xảy ra.

2. 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;

3. Hướng dẫn các CBCCVC của đơn vị trực thuộc Sở 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;

Điều 11. Trách nhiệm của các đơn vị trực thuộc Sở

1. Chấp hành nghiêm túc những chính sách, các quy định về an toàn, an ninh thông tin của Quy định này và các quy định khác của pháp luật. Nâng cao ý thức cảnh giác và trách nhiệm đảm bảo an toàn, an ninh thông tin tại phòng, ban, đơn vị.

2. Khi phát hiện sự cố gây mất an toàn, an ninh thông tin phải báo ngay với Văn phòng Sở để kịp thời ngăn chặn, xử lý.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 12. Khen thưởng và xử lý vi phạm

1. Chánh Văn phòng Sở, Trưởng các đơn vị trực thuộc Sở, CBCCVC có thành tích xuất sắc trong việc thực hiện quy chế này được xét khen thưởng theo quy định.

2. Trường hợp vi phạm Quy chế này thì tùy theo tính chất, mức độ vi phạm bị xử lý theo quy định của pháp luật.

Điều 13. Tổ chức thực hiện Quy chế và sửa đổi, bổ sung Quy chế

1. Văn phòng Sở có trách nhiệm chủ trì phối hợp với các đơn vị trực thuộc Sở hướng dẫn triển khai thực hiện Quy chế này.

2. Trong quá trình thực hiện, nếu có vướng mắc cần điều chỉnh, bổ sung, các đơn vị trực thuộc Sở kịp thời phản ánh bằng văn bản gửi về Văn phòng Sở để tổng hợp trình Giám đốc Sở xem xét, quyết định./.

GIÁM ĐỐC

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

Vũ Nam Tiến