UỶ BAN NHÂN DÂN TỈNH TUYÊN QUANG **SỞ NÔNG NGHIỆP VÀ PTNT**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 246/QĐ - SNN	*Tuyên Quang, ngày 08 tháng 6 năm 2015*

QUYẾT ĐỊNH

Ban hành Quy chế Đảm bảo an toàn, an ninh thông tin và Quản lý ứng dụng công nghệ thông tin của Sở Nông nghiệp và PTNT tỉnh Tuyên Quang

GIÁM ĐỐC SỞ NÔNG NGHIỆP VÀ PTNT TỈNH TUYÊN QUANG

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

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

Căn cứ Chỉ thị số 15/CT-TTg ngày 17/6/2014 của Thủ tướng Chính phủ về tăng cường công tác đảm bảo an ninh và an toàn thông tin mạng trong tình hình mới;

Căn cứ Nghị định số 72/2013/NĐ-CP ngày 15/7/2013 của Chính phủ về Quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng;

Căn cứ Quyết định số 17/2014/QĐ-UBND ngày 21/10/2014 của Ủy ban nhân dân tỉnh Tuyên Quang về Ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước tỉnh Tuyên Quang.

Xét 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 thông tin và Quản lý ứng dụng công nghệ thông tin của Sở Nông nghiệp và PTNT tỉnh Tuyên Quang.

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, Trưởng các phòng, cán bộ, công chức, viên chức và người lao động thuộc Sở Nông nghiệp và PTNT có liên quan chịu trách nhiệm thi hành quyết định này./.

Nơi nhận:
- Như điều 3 (Thực hiện);
- Lãnh đạo Sở;
- Trang TTĐT Sở;
- Lưu VT, VP.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ X.H.C.N VIỆT NAM
SỞ NÔNG NGHIỆP VÀ PHÁT TRIỂN NÔNG THÔN
TỈNH TUYÊN QUANG

Nguyễn Công Nông

QUY CHẾ

Ban hành Quy chế Đảm bảo an toàn, an ninh thông tin và Quản lý ứng dụng công nghệ thông tin của Sở Nông nghiệp và PTNT tỉnh Tuyên Quang

(Ban hành kèm theo Quyết định số 246/QĐ-SNN, ngày 08/6/2015 của Sở Nông nghiệp và PTNT tỉnh Tuyên Quang)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định việc đảm bảo an toàn, an ninh thông tin trong hoạt động công nghệ thông tin(CNTT) và quản lý, ứng dụng công nghệ thông tin và phục vụ công tác điều hành và quản lý hành chính nhà nước nhằm đảm bảo an toàn, an ninh thông tin tại Sở Nông nghiệp và PTNT tỉnh Tuyên Quang.

Điều 2. Đối tượng áp dụng

Quy chế này được áp dụng đối với các phòng chuyên môn, đơn vị trực thuộc Sở Nông nghiệp và PTNT tỉnh Tuyên Quang.

Các cán bộ, công chức, viên chức và người lao động làm việc tại các phòng chuyên môn, đơn vị trực thuộc Sở Nông nghiệp và PTNT thực hiện áp dụng Quy định này trong việc vận hành, khai thác và sử dụng hệ thống thông tin của Sở.

Điều 3. Nguyên tắc áp dụng

1. Quản lý và sử dụng thiết bị CNTT đảm bảo đúng mục đích, phục vụ công việc được giao theo quy định của nhà nước.

2. Sử dụng hệ thống thư điện tử, phần mềm quản lý văn bản để nâng cao việc trao đổi thông tin và hiệu qủa công việc, thúc đẩy cải cách hành chính.

3. Các hoạt động ứng dụng công nghệ thông tin phải đảm bảo an toàn, an ninh thông tin.

4. Những vấn đề không quy định tại Quy chế này thì thực hiện theo quy định tại Quyết định số 17/2014/QĐ-UBND của UBND tỉnh Tuyên Quang và các quy định hiện hành của nhà nước.

Điều 4. Giải thích từ ngữ

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

1. *Thiết bị công nghệ thông tin:* Bao gồm tất cả các loại máy vi tính (máy tính để bàn, máy tính xách tay); các loại thiết bị bên ngoài kết nối với máy vi tính như: máy in, máy quét, máy chiếu, thiết bị lưu trữ thông tin, thiết bị tích điện, thiết bị mạng và các loại thiết bị công nghệ kỹ thuật số khác.

2. *Phần mềm:* Bao gồm tất cả phần mềm hệ thống và phần mềm ứng dụng được cài đặt trên các máy tính.

3. *Mạng cục bộ (LAN):* Là một hệ thống bao gồm các máy tính, máy chủ và các thiết bị ngoại vi được kết nối với nhau thông qua các thiết bị truyền dẫn và thiết bị mạng như thông tin, dữ liệu, phần mềm và các thiết bị ngoại vi.

4. *Tiêu chuẩn công nghệ thông tin:* là các quy định của Nhà nước về các vấn đề liên quan đến ứng dụng công nghệ thông tin.

CHƯƠNG II
QUẢN LÝ, SỬ DỤNG THIẾT BỊ CÔNG NGHỆ THÔNG TIN VÀ MẠNG MÁY TÍNH

Điều 5. Quản lý các thiết bị công nghệ thông tin.

1. Đối với Cơ quan Văn phòng Sở Bộ phận Công nghệ thông tin có trách nhiệm:

a) Quản lý các thiết bị dùng chung, lắp đặt mới và bảo trì, sửa chữa, thiết bị tin học.

b) Quản lý người dùng trong mạng nội bộ LAN của Sở, thực hiện các biện pháp bảo vệ an toàn an ninh mạng. Đảm bảo kết nối mạng LAN ra mạng diện rộng của tỉnh. Cài đặt các phần mềm ứng dụng và quản trị Trang thông tin điện tử của Sở.

c) Hướng dẫn người sử dụng khai thác, bảo quản thiết bị tin học được giao.

2. Các đơn vị trực thuộc Sở có trách nhiệm tổ chức quản lý, sử dụng các thiết bị công nghệ thông tin tại đơn vị mình theo quy định hiện hành.

Điều 6. Tiếp nhận và sử dụng thiết bị CNTT.

1. Đối với cơ quan, đơn vị:

a) Lãnh đạo phòng, đơn vị trực thuộc phải chịu trách nhiệm pháp lý về tất cả thiết bị CNTT được giao cho đơn vị mình quản lý và sử dụng;

b) Phân công người quản lý, sử dụng từng thiết bị CNTT được trang bị;

c) Việc điều chuyển thiết bị tin học trong cơ quan Văn phòng Sở do Lãnh đạo Sở quyết định, đối với các đơn vị trực thuộc do Lãnh đạo đơn vị quyết định, khi điều chuyển phải đảm bảo an toàn dữ liệu và có biên bản giao nhận cả phần cứng, phần mềm và dữ liệu;

d) Máy chủ được đặt tại Bộ phận CNTT của Sở và giao cho Bộ phận CNTT quản lý, vận hành.

2. Các cá nhân được giao sử dụng thiết bị CNTT có trách nhiệm:

a) Không tự ý cài đặt thêm phần mềm không sử dụng cho công việc vào

trong máy tính;

b) Không lưu trữ các thông tin có nội dung bị cấm theo quy định chung của nhà nước, của ngành;

c) Tắt mở máy phải đúng quy trình;

d) Định kỳ sao lưu dữ liệu ra thiết bị lưu trữ ngoài dự phòng. Định kỳ có thể là hằng ngày hoặc tuần tùy theo mức độ phát sinh dữ liệu mới của mỗi người dùng. Việc sao lưu dự phòng này nhằm hạn chế rủi ro mất dữ liệu, khi đĩa cứng gắn bên trong máy tính bị hư ở mức vật lý, không thể khôi phục dữ liệu được;

e) Trong quá trình sử dụng không được tự ý thay đổi linh kiện và thông số kỹ thuật của các thiết bị được cấp. Khi thiết bị có sự cố phải thông báo ngay với cán bộ CNTT biết để hỗ trợ kiểm tra và xử lý. Nếu việc sửa chữa phải cần đến vật tư hoặc kinh phí, cần báo cáo Lãnh đạo sở hoặc Lãnh đạo đơn vị. Trường hợp thiết bị lưu trữ dữ liệu có sự cố kỹ thuật thì tuyệt đối không được đem ra ngoài cơ quan để bảo hành hay sửa chữa. Đối với các thiết bị có dán tem bảo hành đang còn thời hạn thì không được làm rách tem.

Điều 7. Đơn vị, cá nhân sử dụng máy tính trong mạng

1. Chỉ sử dụng máy tính thực hiện những công việc được giao, tuân thủ đúng quy trình kỹ thuật nghiệp vụ, quy trình kỹ thuật vận hành hệ thống công nghệ thông tin.

2. Phải tự chịu trách nhiệm về những sai sót, chậm trễ, mất an toàn do cố ý không tuân thủ quy chế vận hành hệ thống công nghệ thông tin hoặc sự chủ quan của mình gây ra.

3. Khi sử dụng internet phải:

a) Có trách nhiệm bảo vệ hệ thống mạng của cơ quan, cảnh giác với những mặt trái của Internet (virus, hacker, thông tin xấu,…).

b) Chịu trách nhiệm theo quy định của pháp luật nếu bao che hoặc cho người khác sử dụng trang thiết bị, mật khẩu của mình để thực hiện các hành vi phạm pháp.

c) Chịu trách nhiệm về nội dung các thông tin cung cấp, đưa lên mạng và internet.

4. Khi có sự cố đối với hệ thống công nghệ thông tin có trách nhiệm thông báo kịp thời cho cán bộ Công nghệ thông tin để phối hợp xử lý.

Điều 8. Thời gian sử dụng thiết bị tin học

1. Ngoài giờ hành chính hoặc vào ngày nghỉ, lễ, tết cán bộ, công chức, viên chức cần sử dụng thiết bị CNTT để hoàn thành công việc được giao hoặc để học tập, nghiên cứu phải tự chịu trách nhiệm về sự an toàn của tất cả các tài sản có

trong phòng làm việc trong thời gian làm việc ngoài giờ đó.

2. Trong giờ làm việc không được sử dụng thiết bị CNTT vào mục đích cá nhân và các mục đích khác ngoài mục đích công việc.

Điều 9. Quản lý hệ thống mạng

1. Máy chủ và các thiết bị mạng máy tính của Văn phòng Sở Nông nghiệp và PTNT được đặt tại Sở, Văn phòng Sở chịu trách nhiệm quản lý, vận hành:

a) Thực hiện các biện pháp bảo đảm an ninh hệ thống, an toàn dữ liệu, phòng chống virus máy chủ và bảo trì hệ thống.

b) Hỗ trợ người sử dụng trong mạng khi gặp sự cố như: Bị ngắt kết nối mạng, không đăng nhập được vào phần mềm quản lý văn bản, hệ thống thư điện tử, Trang Thông tin điện tử của Sở.

c) Các máy tính trong hệ thống mạng của cơ quan Văn phòng Sở không được kết nối Internet theo đường riêng mà phải kết nối thông qua một cổng ra Internet chung của Sở.

d) Chủ trì phối hợp với các đơn vị trong việc quản lý, sử dụng hệ thống mạng và phát triển hệ thống công nghệ thông tin của Sở.

2. Đối với các máy tính, thiết bị mạng máy tính của các đơn vị trực thuộc Sở do các đơn vị tự quản lý theo quy định.

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

Điều 10. Các biện pháp chung đảm bảo an toàn, an ninh thông tin

1. Đối với các cơ quan, đơn vị:

a) Trang bị đầy đủ các kiến thức bảo mật cơ bản cho cán bộ, công chức, viên chức trước khi cho phép truy nhập và sử dụng hệ thống thông tin;

b) Bố trí cán bộ, công chức, viên chức phụ trách về an toàn hệ thống thông tin (*sau đây gọi tắt là cán bộ phụ trách*). Cán bộ phụ trách được đảm bảo điều kiện học tập, tiếp cận công nghệ, kiến thức an toàn bảo mật thông tin trước khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ;

c) Xác định và phân bổ kinh phí cho các hoạt động liên quan đến việc bảo vệ hệ thống thông tin, thông qua việc đầu tư các thiết bị tường lửa, các chương trình chống thư rác, virus máy tính trên các máy trạm, máy chủ,...và các công việc khác có liên quan đến việc bảo đảm an toàn, an ninh thông tin;

d) Các cơ quan, đơn vị phải bố trí ít nhất 01 máy vi tính riêng, không kết nối mạng nội bộ và Internet dùng để quản lý, lưu giữ, soạn thảo các tài liệu mật

theo quy định. Nghiêm cấm lưu trữ, trao đổi, xử lý, hiển thị thông tin, tài liệu có nội dung bí mật nhà nước, bí mật nội bộ trên mạng viễn thông, Internet không có biện pháp bảo mật theo quy định; kết nối máy tính, thiết bị điện tử có chứa thông tin bí mật nhà nước, bí mật nội bộ vào mạng Internet.

2. Đối với cán bộ phụ trách Công nghệ thông tin tại các cơ quan đơn vị:

a) Tham mưu về các biện pháp bảo đảm an toàn thông tin; vận hành an toàn hệ thống thông tin của đơn vị, triển khai các biện pháp bảo đảm an toàn, an ninh thông tin cho tất cả cán bộ, công chức, viên chức trong đơn vị mình;

b) Khi thực hiện việc cấu hình hệ thống thông tin chỉ cung cấp những chức năng thiết yếu nhất; xác định các chức năng, cổng giao tiếp mạng, giao thức, và dịch vụ không cần thiết để cấm hoặc hạn chế sử dụng;

c) Kiểm soát chặt chẽ việc cài đặt phần mềm vào máy trạm và máy chủ.

3. Đối với cán bộ, công chức, viên chức:

a) Thường xuyên cập nhật chính sách, thủ tục an toàn thông tin của đơn vị và thực hiện hướng dẫn về an toàn, an ninh thông tin của cán bộ phụ trách;

b) Hạn chế việc sử dụng chức năng chia sẻ tài nguyên (*sharing*), nếu sử dụng chức năng này cần bật thuộc tính bảo mật bằng mật khẩu và thực hiện việc thu hồi chức năng này khi đã sử dụng xong;

c) Các máy tính khi không sử dụng trong thời gian dài (*quá 02 giờ làm việc*) cần tắt máy hoặc ngưng kết nối mạng (*trừ hệ thống máy chủ*);

d) Khi mở các tập tin đính kèm theo thư điện tử, nếu biết rõ người gửi thư thì phải lưu tập tin vào máy tính rồi quét virus trước khi mở, không được mở các thư điện tử có tập tin đính kèm có nguồn gốc không rõ ràng để phòng, tránh virus, phần mềm gián điệp đính kèm theo thư;

e) Phải đặt mật khẩu truy nhập vào máy tính của mình, đồng thời thiết lập chế độ bảo vệ màn hình (*screen saver*) có sử dụng mật khẩu bảo vệ sau một khoảng thời gian nhất định không sử dụng máy tính. Khi gắn thiết bị lưu trữ vào máy tính, không được trực tiếp truy cập ngay mà phải quét virus trước;

f) Khi đặt các loại mật khẩu (*tệp tin, máy tính, thư điện tử, tài khoản phần mềm quản lý văn bản,...*) nên nhiều hơn 8 ký tự, có cả số và chữ; đồng thời các loại mật khẩu nên thay đổi sau một khoảng thời gian đưa vào sử dụng (*khoảng sau 01 tháng*), nếu có dấu hiệu lộ phải thay đổi ngay.

Điều 11. Phòng chống Virus

1. Phần mềm, dữ liệu và các phương tiện mang tin khi tiếp nhận từ bên ngoài phải được kiểm tra, diệt virus trước khi sử dụng. Những máy tính phát hiện

có virus phải được tách khỏi mạng về mặt vật lý để tránh tình trạng lây nhiễm sang các máy tính khác.

2. Tất cả các máy tính cần phải được cài phần mềm diệt vi rút và thường xuyên cập nhật phiên bản mới.

3. Tuyệt đối không mở các thư lạ, các tệp tin đính kèm hoặc các liên kết trong các thư lạ. Không vào các trang web không có nguồn gốc xuất xứ rõ ràng.

Điều 12. Chế độ bảo mật dữ liệu

1. Người sử dụng phải chịu trách nhiệm về an ninh, an toàn của dữ liệu khi mình sử dụng hoặc khi được giao lưu trữ. Không được phép cho bất cứ tổ chức, cá nhân nào khai thác, sử dụng dữ liệu lưu trữ nếu không có sự đồng ý của Lãnh đạo Sở.

2. Trong trường hợp có rủi ro hoặc phát hiện nguy cơ xảy ra rủi ro đối với dữ liệu lưu trữ, phải ngừng ngay việc sử dụng các dữ liệu đó và báo ngay cho Cán bộ phụ trách công nghệ thông tin của đơn vị.

3. Cán bộ phụ trách công nghệ thông tin có trách nhiệm áp dụng các biện pháp đảm bảo an ninh, bảo mật những thông tin trên mạng máy tính của cơ quan, đơn vị mình quản lý.

Điều 13. An toàn vật lý

1. Phòng máy chủ phải đảm bảo vệ sinh công nghiệp: không dột, không thấm nước; các trang thiết bị lắp đặt trên sàn kỹ thuật, không bị ánh nắng chiếu rọi trực tiếp; độ ẩm, nhiệt độ đạt tiêu chuẩn quy định cho các thiết bị và máy chủ; trang bị đầy đủ thiết bị phòng chống cháy, nổ, lũ lụt, hệ thống chống sét và hệ thống an ninh chống truy nhập bất hợp pháp.

2. Chương trình, số liệu của đơn vị có khả năng bị lợi dụng phải được loại bỏ khi giao các trang thiết bị có chứa các chương trình, dữ liệu đó cho đơn vị bên ngoài hoặc khi thanh lý tài sản.

Điều 14. An toàn mạng máy tính.

1. Yêu cầu an ninh mạng máy tính

a) Kiểm soát, giám sát được các truy nhập mạng;

b) Ngăn chặn được các truy cập trái phép;

c) Có các biện pháp kỹ thuật, hành chính ngăn chặn việc tiếp cận trái phép các trang thiết bị, đường truyền mạng.

d) Chống mã độc, virus: Lựa chọn, triển khai các phần mềm phòng chống virus, thư rác trên các máy trạm, máy chủ, các thiết bị di động trong mạng và những hệ thống thông tin xung yếu như: Trang thông tin điện tử, Hệ thống thư điện tử, Phần mềm Quản lý văn bản và Điều hành,… để phát hiện, loại trừ những

đoạn mã độc hại. Thường xuyên cập nhật các phiên bản mới, các bản vá lỗi của các phần mềm chống virus, thiết lập chế độ quét tự động thường xuyên ít nhất là hằng tuần.

f) Tổ chức quản lý tài nguyên: Kiểm tra, giám sát chức năng chia sẻ thông tin (*Network File and Folder Sharing*); Người sử dụng khi thực hiện việc chia sẻ tài nguyên trên máy chủ hoặc trên máy cục bộ phải sử dụng mật khẩu để bảo vệ thông tin.

g) Thiết lập cơ chế sao lưu và phục hồi hệ thống:

Hệ thống thông tin phải có cơ chế sao lưu thông tin ở mức người dùng và mức hệ thống, các thông tin sao lưu phải lưu trữ tại nơi an toàn; đồng thời thường xuyên kiểm tra để đảm bảo khả năng phục hồi hệ thống khi có sự cố xảy ra.

h) Xử lý khẩn cấp: Khi phát hiện hệ thống bị tấn công, thông qua các dấu hiệu như luồng tin tăng lên bất ngờ, nội dung trang chủ Web bị thay đổi, hệ thống hoạt động rất chậm khác thường,... cần thực hiện các bước cơ bản sau:

Bước 1: Ngắt kết nối máy chủ ra khỏi mạng;

Bước 2: Sao chép logfile và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ (*phục vụ cho công tác phân tích*);

Bước 3: Khôi phục hệ thống bằng cách sử dụng dữ liệu backup mới nhất để hệ thống hoạt động.

2. Trách nhiệm người sử dụng mạng:

a) Khi phát hiện thấy dấu hiệu mất an toàn, phải thông báo ngay cho người quản trị mạng xử lý;

b) Chấp hành các quy định khác của đơn vị phù hợp với các quy định tại Quy chế này.

3. Cán bộ phụ trách Công nghệ thông tin thực hiện các nội dung sau:

a) Thường xuyên kiểm tra, đảm bảo mạng máy tính hoạt động liên tục, ổn định và an toàn;

b) Quản lý cấu hình mạng, tài nguyên và người sử dụng trên mạng;

c) Thiết lập đầy đủ các chế độ kiểm soát an ninh mạng. Sử dụng các công cụ được trang bị, dò tìm và phát hiện kịp thời các điểm yếu, dễ bị tổn thương và các truy nhập bất hợp pháp vào hệ thống mạng. Thường xuyên xem xét, phát hiện những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào mạng;

d) Phát hiện, xử lý kịp thời những lỗ hổng về an ninh của hệ thống mạng;

e) Hướng dẫn, hỗ trợ người sử dụng bảo vệ tài khoản, tài nguyên trên mạng, cài đặt các phần mềm chống và diệt virus và giải quyết kịp thời những sự cố truy nhập mạng;

f) Kiểm tra và ngắt kết nối ra khỏi mạng những máy tính của người sử dụng không tuân thủ các quy định của đơn vị về phòng, chống virus và các quy định khác về an ninh mạng.

CHƯƠNG IV
TỔ CHỨC THỰC HIỆN

Điều 15. Khen thưởng và xử phạt

Việc thực hiện Quy chế này được coi là một trong số những nội dung để xem xét, thi đua khen thưởng hàng năm. Đơn vị, cá nhân nào vi phạm thì tùy theo tính chất, mức độ vi phạm sẽ xử lý kỷ luật hoặc các hình thức xử lý khác theo quy định của pháp luật; nếu vi phạm gây thiệt hại đến tài sản, thiết bị, thông tin, sữ liệu trên mạng máy tính phải chịu trách nhiệm bồi thường theo quy định của pháp luật.

Điều 16. Tổ chức thực hiện

1. Đơn vị, cá nhân sử dụng mạng máy tính và các thiết bị công nghệ trong hệ thống công nghệ thông tin của Sở Nông nghiệp và PTNT có trách nhiệm thi hành Quy chế này.

2. Lãnh đạo các đơn vị, Trưởng các phòng chức năng thuộc Sở có trách nhiệm tổ chức triển khai và kiểm tra việc chấp hành tại đơn vị mình theo đúng Quy chế này.

Trong quá trình thực hiện nếu có phát sinh khó khăn, vướng mắc cần sửa đổi, bổ sung các phòng, đơn vị kịp thời báo cáo bằng văn bản về Văn phòng Sở để tổng hợp, báo cáo Lãnh đạo Sở xem xét điều chỉnh bổ sung./.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ X.H.C.N VIỆT NAM
SỞ NÔNG NGHIỆP VÀ PHÁT TRIỂN NÔNG THÔN
TỈNH TUYÊN QUANG

Nguyễn Công Nông