UBND TỈNH TUYÊN QUANG **SỞ TƯ PHÁP**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 193/QĐ-STP	*Tuyên Quang, ngày 11 tháng 11 năm 2020*

QUYẾT ĐỊNH
Ban hành Quy chế Đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Sở Tư pháp tỉnh Tuyên Quang

GIÁM ĐỐC SỞ TƯ PHÁP TỈNH TUYÊN QUANG

Căn cứ Luật Giao dịch điện tử ngày 29 tháng 11 năm 2005;

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 Nghị định số 72/2013/NĐ-CP ngày 15/7/2013 của Chính phủ về quản lý, cung cấp và 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 việc 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;

Căn cứ Quyết định số 222/QĐ-UBND ngày 28/7/2015 của Ủy ban nhân dân tỉnh Tuyên Quang về việc quy định chức năng, nhiệm vụ, quyền hạn, tổ chức bộ máy của Sở Tư pháp tỉnh Tuyên Quang; Quyết định số 330/QĐ-UBND ngày 25/9/2017 của ủy ban nhân dân tỉnh Tuyên Quang về việc sửa đổi, bổ sung quyết định quy định về chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Văn phòng UBND tỉnh, Sở Tư pháp, Sở Nội vụ; Quyết định số 104/QĐ-UBND ngày 01 tháng 4 năm 2020 của Ủy ban nhân dân tỉnh Tuyên Quang về việc sắp xếp lại cơ cấu tổ chức của Sở Tư pháp tỉnh Tuyên Quang;

Theo đề nghị của Trưởng Phòng Xây dựng, kiểm tra, theo dõi thi hành pháp luật và phổ biến, giáo dục pháp luật.

QUYẾT ĐỊNH:

Điều 1. Ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Sở Tư pháp tỉnh Tuyên Quang (Có Quy

chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Sở Tư pháp tỉnh Tuyên Quang kèm theo).

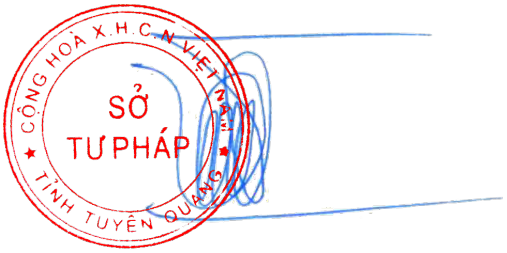
Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Điều 3. Các ông, bà: Chánh Văn phòng Sở; Chánh Thanh tra Sở; Trưởng phòng, thủ trưởng đơn vị thuộc Sở và trực thuộc Sở; công chức, viên chức, người lao động Sở Tư pháp; tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- UBND tỉnh (b/cáo);
- Sở TT&TT;
- Giám đốc Sở;
- Các PGĐ Sở;
- Như Điều 3 (thực hiện);
- Lưu VT.

Đ.Thành-03

GIÁM ĐỐC



Nguyễn Thị Thược

UBND TỈNH TUYÊN QUANG
SỞ TƯ PHÁP

CỘNG HOÀ 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 của Sở Tư pháp tỉnh Tuyên Quang

(ban hành kèm theo Quyết định số 193/QĐ-STP ngày 11 tháng 11 năm 2020 của Giám đốc Sở Tư pháp tỉnh Tuyên Quang)

Chương I
NHỮNG 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 ứng dụng công nghệ thông tin của Sở Tư pháp tỉnh Tuyên Quang.

Điều 2. Đối tượng áp dụng

Quy chế này được áp dụng đối với các phòng, đơn vị thuộc Sở, đơn vị sự nghiệp trực thuộc Sở; công chức, viên chức, người lao động Sở Tư pháp tỉnh Tuyên Quang trong việc quản lý, khai thác, sử dụng và đảm bảo an toàn, an ninh thông tin của Sở.

Điều 3. Nguyên tắc áp dụng

Những nội dung liên quan đến việc quản lý, sử dụng, đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin không quy định tại Quy chế này, thì thực hiện theo quy định của pháp luật hiện hành, các quy định, quy chế khác của Sở Tư pháp.

Chương II
TRÁCH NHIỆM QUẢN LÝ, SỬ DỤNG, ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 4. Phân loại tài nguyên của hệ thống thông tin

1. Hệ thống thông tin của Sở Tư pháp được phân loại thành 03 loại tài nguyên chính, bao gồm:

a) Tài nguyên về dữ liệu.

b) Tài nguyên về phần mềm.

c) Tài nguyên về phần cứng.

2. Trong 03 loại tài nguyên quy định tại khoản 1 Điều này, tài nguyên về dữ liệu trong hệ thống thông tin quy định tại điểm a được ưu tiên bảo vệ ở mức độ cao nhất.

Điều 5. Trách nhiệm của công chức, viên chức, người lao động trong quản lý, khai thác, sử dụng hệ thống thông tin

1. Tuân thủ nghiêm các quy định của nhà nước, của Sở Tư pháp về đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin.

2. Không được chơi các trò chơi trực tuyến *(game online)* hoặc các trò chơi khác trên Internet trong giờ làm việc.

3. Không được truy cập hoặc tải các trang website có nội dung đồi trụy, phản động, các chương trình không rõ nguồn gốc, các thông tin quảng cáo.

4. Khi sử dụng hệ thống thư điện tử (Email), không được kích chuột vào bất cứ thư điện tử, tệp đính kèm, đường link, thư rác, thư quảng cáo nào không rõ nguồn gốc và không xác định được người gửi.

Điều 6. Quản lý thiết bị công nghệ thông tin

1. Thiết bị công nghệ thông tin được trang bị tại các phòng, đơn vị và giao cho cá nhân quản lý, sử dụng là tài sản của Nhà nước, được quản lý, sử dụng theo quy định của pháp luật và của Sở Tư pháp tỉnh Tuyên Quang. Các phòng, đơn vị, công chức, viên chức, người lao động có trách nhiệm quản lý trang thiết bị được giao đảm bảo đúng mục đích, đúng quy định.

2. Phòng Xây dựng, kiểm tra, theo dõi thi hành pháp luật và phổ biến, giáo dục pháp luật thực hiện chức năng, nhiệm vụ quản trị mạng, trực tiếp quản lý kỹ thuật và duy trì hoạt động của hệ thống thông tin; là đầu mối kết nối mạng LAN, mạng Internet, mạng dữ liệu chuyên dùng; kiểm tra hiện trạng, đề xuất sửa chữa hoặc mua mới các chủng loại thiết bị công nghệ thông tin phù hợp, an toàn, bảo mật theo quy định về quản lý, sử dụng tài sản cho các phòng, đơn vị thuộc Sở.

3. Các đơn vị sự nghiệp trực thuộc Sở cử một đầu mối thực hiện các nhiệm vụ quy định tại khoản 2 Điều này tại đơn vị mình.

Điều 7. Quản lý, khai thác, sử dụng phần mềm

1. Phòng Xây dựng, kiểm tra, theo dõi thi hành pháp luật và phổ biến, giáo dục pháp luật có trách nhiệm cài đặt, quản lý các phần mềm hệ thống và phần mềm ứng dụng trong hệ thống mạng máy tính tại các phòng, đơn vị thuộc Sở, công chức, người lao động thuộc các phòng, đơn vị chuyên môn thuộc Sở; Nghiên cứu, đề xuất, nâng cấp công nghệ, phần mềm theo định hướng quản lý nhà nước của ngành và tuân theo quy định của pháp luật.

2. Các phòng, đơn vị, công chức, viên chức, người lao động có trách nhiệm phối hợp với Phòng Xây dựng, kiểm tra, theo dõi thi hành pháp luật và

phổ biến, giáo dục pháp luật, chuyên viên quản trị mạng trong quá trình triển khai, khai thác và sử dụng các phần mềm do Sở Tư pháp triển khai, ứng dụng.

3. Phần mềm, cơ sở dữ liệu chuyên ngành thuộc lĩnh vực chuyên môn của phòng, đơn vị nào thì do phòng, đơn vị đó quản lý, khai thác và sử dụng; Trưởng phòng, thủ trưởng đơn vị chịu trách nhiệm phân công cho từng cá nhân quản lý, sử dụng, khai thác theo quy định. Đối với các phần mềm dùng chung như: Hệ thống quản lý văn bản và điều hành, Hệ thống một cửa điện tử của tỉnh/quốc gia do Phòng Xây dựng, kiểm tra, theo dõi thi hành pháp luật và phổ biến, giáo dục pháp luật quản trị tài khoản người dùng; công chức, viên chức, người lao động trong cơ quan được cấp tài khoản cá nhân để khai thác, sử dụng.

Điều 8. Bảo mật cơ sở dữ liệu, an ninh mạng và phòng chống virus máy tính

1. Bảo mật dữ liệu: Công chức, viên chức, người lao động có trách nhiệm bảo mật dữ liệu trên các thiết bị công nghệ thông tin được giao quản lý, sử dụng. Việc chia sẻ dữ liệu trên mạng do bộ phận quản trị mạng thực hiện theo quyết định của Giám đốc Sở và theo phân cấp sử dụng tài nguyên mạng.

2. Bảo mật truy cập: Các thiết bị công nghệ thông tin, phần mềm ứng dụng, cơ sở dữ liệu phải được đặt mật khẩu truy cập.

3. Bảo mật hệ thống mạng và truyền tin: Mạng và đường truyền được áp dụng các chế độ bảo mật cần thiết, chống xâm nhập bất hợp pháp. Bộ phận quản trị mạng có trách nhiệm thường xuyên theo dõi, kiểm tra phát hiện kịp thời các hoạt động xâm nhập và có biện pháp xử lý kịp thời.

4. An toàn trong sử dụng: Khi không làm việc với thiết bị công nghệ thông tin trong thời gian dài, công chức, viên chức, người lao động thuộc Sở phải tắt hoặc đặt chế độ bảo vệ để đảm bảo an toàn.

5. Phòng, chống virus: Công chức, viên chức, người lao động thuộc Sở có trách nhiệm tuân thủ các biện pháp phòng chống virus, phần mềm độc hại trên các thiết bị công nghệ thông tin, đảm bảo an toàn dữ liệu được giao quản lý. Mọi dữ liệu từ các thiết bị lưu trữ bên ngoài đều phải được quét, diệt virus trước khi đưa vào máy. Những máy tính phát hiện có virus, phần mềm độc hại phải được tách khỏi mạng về mặt vật lý để tránh tình trạng lây nhiễm sang các máy tính khác. Không truy cập vào các link liên kết không rõ ràng; không click vào các link, tải về các file tài liệu từ các địa chỉ thư không biết rõ thông tin, địa chỉ người gửi.

Điều 9. Đảm bảo an toàn máy chủ, máy trạm, các thiết bị di động và cơ chế sao lưu, phục hồi

1. Kiểm soát chặt chẽ việc cài đặt các phần mềm mới lên máy chủ, máy trạm và các thiết bị di động. Các phần mềm được cài đặt trên máy chủ, máy trạm và các thiết bị di động *(bao gồm hệ điều hành, các phần mềm ứng dụng văn phòng, phần mềm phục vụ công việc, tiện ích khác)* phải được thường xuyên theo dõi, cập nhật bản vá lỗi bảo mật của nhà phát triển, cài đặt các phần mềm phòng chống virus, mã độc và thường xuyên cập nhật phiên bản mới, đặt lịch quét virus theo định kỳ.

2. Cơ chế sao lưu, phục hồi máy chủ, máy trạm

Dữ liệu phát sinh trong quá trình vận hành các phần mềm ứng dụng, cơ sở dữ liệu chuyên ngành của Sở Tư pháp phải được sao lưu định kỳ 01 lần/tuần hoặc sao lưu đột xuất theo yêu cầu quản lý nhằm phục vụ cho việc phục hồi, khắc phục hệ thống kịp thời khi có sự cố xảy ra.

Công chức, viên chức, người lao động có trách nhiệm sao lưu định kỳ hoặc sao lưu đột xuất theo chỉ đạo của Giám đốc Sở dữ liệu công việc do cá nhân quản lý.

Điều 10. Đảm bảo an toàn hệ thống mạng máy tính, kết nối Internet

1. Quản lý hệ thống mạng nội bộ

Mạng nội bộ của Sở được tổ chức theo mô hình Clients/Server; mạng nội bộ khi kết nối với mạng Internet phải thông qua thiết bị tường lửa kiểm soát, có phân chia hệ thống mạng nội bộ thành các vùng mạng theo phạm vi truy cập, vô hiệu hóa tất cả các dịch vụ không sử dụng tại từng vùng mạng, thực hiện nguyên tắc chỉ mở các dịch vụ cần thiết khi có yêu cầu.

2. Quản lý hệ thống mạng không dây (wifi)

Mạng không dây (wifi) của Sở được phân tách thành lớp mạng riêng. Khi thiết lập mạng không dây có kết nối vào mạng nội bộ phải thiết lập các thông số cần thiết như định danh, mật mã, mã hóa dữ liệu, có thay đổi mật mã định kỳ.

3. Quản lý truy cập từ xa vào mạng nội bộ

Đối với việc truy cập từ xa vào mạng nội bộ phải được theo dõi, quản lý chặt chẽ, nhất là truy cập có sử dụng chức năng quản trị, phải thiết lập mật mã độ an toàn cao, thường xuyên thay đổi mật mã, hạn chế truy cập từ xa vào mạng nội bộ từ các điểm truy cập Internet công cộng.

Điều 11. Đảm bảo an toàn truy cập, đăng nhập hệ thống thông tin

1. Mỗi công chức, viên chức, người lao động được cấp và sử dụng tài khoản truy cập với định danh duy nhất gắn với người dùng đó để truy cập, đăng nhập các hệ thống thông tin của Sở. Trường hợp sử dụng tài khoản dùng chung cho một nhóm người hay một đơn vị, bộ phận phải có cơ chế xác định được cá nhân có trách nhiệm quản lý tài khoản. Công chức, viên chức, người lao động chỉ được truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình và có trách nhiệm bảo mật tài khoản truy cập được cấp.

2. Mật mã đăng nhập, truy cập hệ thống thông tin phải có độ phức tạp cao *(có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự in hoa, ký tự số hoặc ký tự đặc biệt như !, @, #, $, %,...)*.

Điều 12. Đảm bảo an toàn thông tin, dữ liệu

1. Thông tin, dữ liệu khi được lưu trữ, khai thác, trao đổi phải được đảm bảo tính toàn vẹn, tính tin cậy, tính sẵn sàng. Thông tin, dữ liệu quan trọng khi

được lưu trữ, trao đổi phải áp dụng kỹ thuật mã hóa, thiết lập mật khẩu, ứng dụng chữ ký số và phải có cơ chế lưu trữ dự phòng.

2. Trong trao đổi thông tin, dữ liệu phục vụ công việc, công chức, viên chức, người lao động động phải sử dụng Hệ thống quản lý văn bản và điều hành, hệ thống thư điện tử công vụ *(@tuyenquang.gov.vn)*. Hạn chế việc sử dụng các phương tiện trao đổi thông tin dữ liệu, hệ thống thư điện tử công cộng, mạng xã hội trên Internet trong hoạt động của cơ quan.

Điều 13. Xử lý khẩn cấp

Khi phát hiện hệ thống bị tấn công, thông qua các các dấu hiệu như: luồng thông tin tăng lên bất ngờ, nội dung trang chủ trang thông tin điện tử bị thay đổi, hệ thống hoạt động chậm khác thường và các dấu hiệu khác, chuyên viên quản trị mạng cần thực hiện ngay các bước sau:

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

2. 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)*;

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

4. Bước 4: Báo cáo Giám đốc Sở và Sở Thông tin và Truyền thông bằng văn bản. Trường hợp có sự cố nghiêm trọng vượt quá khả năng khắc phục, phải báo cáo ngay Giám đốc Sở để chỉ đạo; đề nghị Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ.

Chương III
TỔ CHỨC THỰC HIỆN

Điều 14. Điều khoản thi hành

1. Các phòng, đơn vị thuộc Sở, đơn vị sự nghiệp trực thuộc Sở, công chức, viên chức, người lao động Sở Tư pháp có trách nhiệm thực hiện nghiêm túc Quy chế này.

2. Trong quá trình thực hiện, nếu có vấn đề phát sinh hoặc khó khăn, vướng mắc, các phòng, đơn vị, cá nhân phản ánh kịp thời về Phòng Xây dựng, kiểm tra, theo dõi thi hành pháp luật và phổ biến, giáo dục pháp luật để tổng hợp, báo cáo Giám đốc Sở xem xét quyết định./.

GIÁM ĐỐC

CỘNG HOÀ X.H.C.N VIỆT NAM
SỞ TƯ PHÁP
TỈNH TUYÊN QUANG

Nguyễn Thị Thược