UBND TỈNH THỪA THIÊN HUẾ
SỞ TƯ PHÁP

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

Số: 159/QĐ-STP

Thừa Thiên Huế, ngày 18 tháng 11 năm 2021

QUYẾT ĐỊNH
Ban hành Quy chế đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của Sở Tư pháp tỉnh Thừa Thiên Huế

GIÁM ĐỐC SỞ TƯ PHÁP TỈNH THỪA THIÊN HUẾ

Căn cứ Luật Công nghệ thông tin số 67/2006/QH11;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 04 năm 2007 của Thủ tướng Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Căn cứ Quyết định 2072/QĐ-UBND ngày 16 tháng 10 năm 2014 của Ủy ban nhân dân tỉnh quy định về việc đảm bảo an toàn, an ninh thông tin trên môi trường mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Thừa Thiên Huế;

Căn cứ Quyết định số 20/2021/QĐ-UBND ngày 03 tháng 4 năm 2021 của Ủy ban nhân dân tỉnh Thừa Thiên Huế ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Tư pháp tỉnh Thừa Thiên Huế;

Theo đề nghị của Trưởng phòng Phổ biến, giáo dục pháp luật.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế về đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của Sở Tư pháp tỉnh Thừa Thiên Huế.

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

Điều 3. Trưởng Phòng Phổ biến, giáo dục pháp luật, Chánh Văn phòng; Trưởng các phòng chuyên môn, Thủ trưởng các cơ quan, đơn vị thuộc Sở; công chức, viên chức và người lao động thuộc Sở Tư pháp tỉnh chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như điều 3;
- Lãnh đạo Sở;
- Lưu: VT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ TƯ PHÁP
TỈNH THỪA THIÊN HUẾ

Nguyễn Thanh Sơn

UBND TỈNH THỪA THIÊN HUẾ
SỞ TƯ PHÁP

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

QUY CHẾ

Về việc đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của Sở Tư pháp

(Ban hành kèm theo Quyết định số 159/QĐ-STP ngày 18 tháng 11 năm 2021 của Sở Tư pháp tỉnh Thừa Thiên Huế)

Chương I

NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. 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 của Sở Tư pháp.

2. Quy chế này được áp dụng với tất cả công chức, viên chức và người lao động thuộc Sở Tư pháp.

Điều 2. Mục đích, nguyên tắc đảm bảo an toàn thông tin

1. Việc áp dụng Quy chế này nhằm giảm thiểu được các nguy cơ gây mất an toàn thông tin và đảm bảo an ninh thông tin trong quá trình ứng dụng công nghệ thông tin trong hoạt động của Sở Tư pháp.

2. Các hoạt động ứng dụng công nghệ thông tin phải tuân thủ theo nguyên tắc đảm bảo an toàn thông tin được quy định tại Quyết định 2072/QĐ-UBND ngày 16 tháng 10 năm 2014 của UBND tỉnh quy định về việc đảm bảo an toàn, an ninh thông tin trên môi trường mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Thừa Thiên Huế.

Chương II

QUY ĐỊNH ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 3. Các hành vi nghiêm cấm

1. Không được tự ý gỡ bỏ các phần mềm phòng chống virus và phòng chống mã độc trên máy tính. Các phần mềm trên phải được thiết lập chế độ tự động cập nhật. Tất cả các tập tin, thư mục khi sao chép vào máy tính từ thiết bị bên ngoài phải được quét mã độc trước khi sao chép, sử dụng.

2. Không tự ý thay đổi, tháo lắp các thiết bị trên máy tính.

3. Không bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của đơn vị, cá nhân khác.

4. Nghiêm cấm sử dụng các hộp thư điện tử công cộng (Yahoo, Gmail, Hotmail ...) để trao đổi công việc của cơ quan.

5. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm mã độc trên máy tính (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu,…), người sử dụng phải tắt máy và báo trực tiếp cho cán bộ chuyên trách công nghệ thông tin (CNTT) để kịp thời xử lý.

6. Nghiêm cấm tạo ra, cài đặt, phát tán vi rút máy tính, phần mềm độc hại trái pháp luật.

Điều 4. Quản lý truy cập mạng LAN và WIFI

1. Địa chỉ IP và địa chỉ Default Gateway là định danh duy nhất của máy tính cá nhân khi tham gia mạng nội bộ, mỗi cá nhân sử dụng máy tính trong mạng nội bộ không tự ý thay đổi các địa chỉ IP và địa chỉ Default gateway đã được cấp

2. Mỗi tài khoản truy cập các hệ thống thông tin chỉ được cấp cho một người quản lý và sử dụng. Do đó người sử dụng phải có trách nhiệm bảo mật tài khoản truy cập của mình.

3. Việc sử dụng mạng riêng ảo (VPN - Virtual Private Network) khi có nhu cầu làm việc từ xa, yêu cầu người sử dụng đặt mật khẩu với độ an toàn cao, nên thay đổi mật khẩu thường xuyên.

4. Hạn chế việc sử dụng chức năng chia sẻ tài nguyên (sharing) trừ máy in, khi sử dụng chức năng này cần có chức năng bảo mật bằng mật khẩu và thực hiện việc thu hồi chức năng này khi đã sử dụng xong.

Điều 5. Sử dụng các Hệ thống thông tin và Thư điện tử công vụ

1. Không xâm nhập, sửa đổi, xóa bỏ nội dung thông tin của đơn vị, cá nhân khác.

2. Mỗi công chức, viên chức và người lao động phải tự đặt mật khẩu đăng nhập vào các Hệ thống thông tin và Thư điện tử công vụ có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số và ký tự đặc biệt như !, @, #, $, %,...) và thường xuyên thay đổi nhằm tăng cường công tác bảo mật.

3. Không được truy cập vào các Trang thông tin điện tử không rõ về nội dung. Không đọc những thư điện tử không rõ nguồn gốc người gửi và kích hoạt các đường liên kết có dấu hiệu không rõ ràng.

4. Không tải những file đính kèm trên thư điện tử công vụ và các Trang thông tin khác không rõ nguồn gốc.

5. Nghiêm cấm việc lợi dụng Hệ thống thông tin để cung cấp, truyền đi, quảng bá hoặc đặt đường liên kết trực tiếp đến những thông tin chống lại nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam.

6. Nghiêm cấm đăng phát các hình ảnh phản cảm, thiếu tính nhân văn không phù hợp với thuần phong, mỹ tục Việt Nam.

7. Đối với các cá nhân nghỉ việc, chuyển công tác, cán bộ chuyên trách CNTT làm Công văn gửi Sở Thông tin và Truyền thông để hủy tài khoản, xóa quyền truy cập các hệ thống thông tin, thiết lập thư điện tử công đúng quy định.

Điều 6. Cài đặt các phần mềm ứng dụng

1. Các phần mềm Windows, Microsoft Office, phần mềm phục vụ đối thoại trên mạng (yahoo, skype…), phần mềm gõ tiếng việt, các trình duyệt web và một số phần mềm phục vụ cho công việc văn phòng của từng cá nhân (xử lý ảnh, kế toán, lập trình…) được cài đặt trên máy tính để bàn, laptop.

2. Nghiêm cấm việc cài đặt các phần mềm không có nguồn gốc xuất xứ trên máy tính cơ quan. Nếu tải trên mạng những ứng dụng thông dụng được nêu tại Khoản 1 Điều này phải tìm các kho dữ liệu có uy tín không bị kèm theo mã độc.

3. Không tải và cài đặt các phần mềm không liên quan đến công việc chuyên môn lên máy tính cơ quan.

Điều 7. Quản lý sự cố

1. Phân loại mức độ nghiêm trọng của các sự cố, bao gồm:

a) Thấp: Sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của các phòng, đơn vị thuộc Sở Tư pháp.

b) Trung bình: Sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoán hay đình trệ hoạt động chính của các phòng, đơn vị thuộc Sở Tư pháp.

c) Cao: Sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và gây ảnh hưởng đến một trong các hoạt động chính của các phòng, đơn vị thuộc Sở Tư pháp.

d) Khẩn cấp: Sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của các phòng, đơn vị thuộc Sở Tư pháp.

2. Xử lý sự cố:

Khi có sự cố thì công chức, viên chức, người lao động phải báo với chuyên trách CNTT để kịp thời xử lý.

Đối với sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của Sở Tư pháp thì chuyên trách CNTT báo cáo ngay cho Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ.

Điều 8. Nhiệm vụ của Chuyên trách CNTT

1. Có trách nhiệm thiết lập mạng không dây trong nội bộ đơn vị, đặt mật khẩu truy cập, chịu trách nhiệm thay đổi và quản lý mật khẩu.

2. Các thiết bị mạng quan trọng như tường lửa (firewall), thiết bị định tuyến (router),… phải được đặt trong phòng máy chủ và có các biện pháp bảo vệ, ngăn chặn xâm nhập trái phép vào phòng máy chủ.

3. Giám sát, nhắc nhở, khuyến cáo công chức, viên chức, người lao động thay đổi mật khẩu thường xuyên.

4. Tổ chức hướng dẫn, tập huấn về phòng chống mã độc, các rủi ro do mã độc gây ra cho công chức, viên chức, người lao động trong toàn cơ quan.

5. Thường xuyên cập nhật Quy định an toàn an ninh thông tin trong quá trình vận hành phòng hệ thống.

6. Cung cấp dữ liệu điện tử của các đoàn thanh tra, đoàn tham mưu giải quyết khiếu nại, tố cáo khi người có thẩm quyền yêu cầu.

7. Triển khai các giải pháp tổng thể bảo đảm an toàn, an ninh thông tin mạng trong toàn hệ thống; các giải pháp kỷ thuật phòng chống virut, mã độc, thư rác cho hệ thống và máy tính cá nhân cho công chức, viên chức, người lao động trong cơ quan.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 9. Trách nhiệm của cán bộ, công chức và người lao động trong cơ quan

1. Nghiêm túc chấp hành 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 công chức, viên chức, người lao động phải có trách nhiệm tự quản lý, bảo quản thiết bị đã được giao sử dụng.

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

4. Tham gia các chương trình tập huấn về an toàn an ninh thông tin do cơ quan tổ chức.

5. Việc soạn thảo, đánh máy, in, sao chụp tài liệu mật phải thực hiện đúng quy định của pháp luật về bảo vệ bí mật nhà nước.

6. Các máy tính khi không sử dụng trong thời gian dài quá 02 giờ trở lên cần tắt máy, để tránh bị các hacker lợi dụng, sử dụng chức năng điều khiển từ xa dùng máy tính của mình tấn công vào các hệ thống thông tin khác.

7. Không cung cấp mật khẩu cho người ngoài trừ những đoàn công tác đến làm việc trực tiếp với đơn vị.

Điều 10. Trách nhiệm của các phòng, đơn vị sự nghiệp thuộc Sở

1. Trưởng phòng, Thủ trưởng đơn vị sự nghiệp có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trong công tác đảm bảo an toàn thông tin của phòng, đơn vị mình.

2. 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.

3. Phân công một chuyên viên thường xuyên theo dõi để đảm bảo an toàn thông tin của phòng, đơn vị.

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.

Chương IV

TỔ CHỨC THỰC HIỆN

Điều 12. Khen thưởng và xử lý vi phạm

1. Việc thực hiện tốt quy chế này là một tiêu chuẩn để xem xét đánh giá thi đua của mỗi cá nhân, đơn vị.

2. Các phòng, đơn vị thuộc Sở Tư pháp; công chức, viên chức, người lao động có hành vi vi phạm quy chế này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật theo trách nhiệm hoặc bị truy cứu trách nhiệm hình sự. Nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật hiện hành.

3. Trong quá trình thực hiện nếu có phát sinh khó khăn, vướng mắc cần sửa đổi, bổ sung các phòng kịp thời thông tin cho chuyên trách CNTT tổng hợp báo cáo Lãnh đạo Sở xem xét, giải quyết./.

SỞ TƯ PHÁP TỈNH THỪA THIÊN HUẾ