UBND TỈNH THỪA THIÊN HUẾ **THANH TRA TỈNH**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 806 /QĐ-TTr	*Thừa Thiên Huế, ngày 05 tháng 9 năm 2018*

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 Thanh tra tỉnh Thừa Thiên Huế

CHÁNH THANH TRA TỈNH

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19/6/2015;

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

Căn cứ Luật An toàn thông tin mạng ngày 19/11/2015;

Căn cứ Nghị định 85/2016/NĐ-CP ngày 01/7/2016 quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ;

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

Căn cứ Quyết định 2072/QĐ-UBND ngày 16/10/2014 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;

Căn cứ Quyết định số 31/2016/QĐ-UBND ngày 18/5/2016 của UBND tỉnh Thừa Thiên Huế về việc Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Thanh tra tỉnh;

Theo đề nghị của Chánh Văn phòng Thanh tra tỉnh,

QUYẾT ĐỊNH:

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

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký và thay thế Quy chế đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của Thanh tra tỉnh Thừa Thiên Huế ban hành kèm theo Quyết định 514/QĐ-TTr ngày 20/7/2015 của Thanh tra tỉnh.

Điều 3. Chánh Văn phòng, các Trưởng phòng Thanh tra, giải quyết khiếu nại, tố cáo 1, 2, 3; Trưởng phòng Thanh tra phòng, chống tham nhũng, Trưởng phòng Giám sát, kiểm tra và Xử lý sau thanh tra và các công chức, viên chức có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- UBND tỉnh;
- Sở TT&TT;
- Đăng tải: Trang TTĐT;
- Lưu: VT.

CHÁNH THANH TRA

Ký bởi: Thanh Tra tỉnh
Email: @thuathienhue.gov.vn
Cơ quan: Tỉnh Thừa Thiên Huế
Thời gian ký: 5.9.2018 15:25

UBND TỈNH THỪA THIÊN HUẾ
THANH TRA TỈNH

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

QUY CHẾ
Đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của Thanh tra tỉnh Thừa Thiên Huế

(Ban hành kèm theo Quyết định số 806 /QĐ-TTr ngày 05 tháng 9 năm 2018 của Chánh Thanh tra tỉnh)

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 thông suốt, an toàn, bảo mật thông tin trong hoạt động ứng dụng công nghệ thông tin (CNTT) vào việc quản lý, sử dụng, lưu trữ, truyền đưa thông tin của Thanh tra tỉnh trên môi trường mạng.

2. Quy chế này được áp dụng với tất cả cán bộ, công chức và người lao động (CBCC) thuộc Thanh tra tỉnh.

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 Thanh tra tỉnh.

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 16/10/2014 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 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.

7. Sử dụng máy tính hoặc các thiết bị khác có kết nối mạng internet để soạn thảo, đánh máy, lưu giữ thông tin, tài liệu, thiết bị mang bí mật nhà nước; cắm thiết bị lưu giữ bí mật nhà nước vào máy tính có kết nối mạng internet.

Điều 4. Quản lý truy cập mạng LAN và WiFi

1. Mạng LAN cơ quan được kết nối với hệ thống mạng diện rộng tỉnh bằng CPNet và truy cập Internet tập trung phục vụ công việc.

2. Địa chỉ IP và địa chỉ Default gateway của mỗi CBCC là định danh duy nhất của máy tính cá nhân khi tham gia mạng nội bộ và được cấp theo danh sách Phụ lục 1 đính kèm. 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.

3. Máy tính kết nối vào mạng LAN cơ quan khuyến nghị đặt mật khẩu với độ an toàn cao, nên thay đổi mật khẩu thường xuyên để đảm bảo an toàn thông tin cho mỗi cá nhân.

4. 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.

5. 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.

6. Mạng Wifi được thiết lập độc lập với hệ thống mạng LAN của cơ quan, phục vụ cho nhu cầu tra cứu thông tin và phục vụ người dân, tổ chức đến liên hệ công tác.

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 CBCC 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 phải được thay đổi ít nhất **3 tháng/lần** 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 hưu, nghỉ việc, chuyển công tác, cán bộ chuyên trách CNTT làm Công văn gửi Sở Thông tin và Truyền thông (TT&TT) để hủy tài khoản, xóa quyền truy cập các hệ thống thông tin, thư điện tử công vụ 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 (Zalo, 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 như BKAV, Symantec…

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 thuộc Thanh tra tỉnh.

b) Trung bình: Sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của các phòng thuộc Thanh tra tỉnh.

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 thuộc Thanh tra tỉnh.

d) Khẩn cấp: Sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của các phòng thuộc Thanh tra tỉnh.

2. Xử lý sự cố:

Khi có sự cố thì CBCC phải báo với cán bộ 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 Thanh tra tỉnh thì cán bộ chuyên trách CNTT báo cáo ngay cho Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 8. Nhiệm vụ của cán bộ 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 theo định kỳ.

2. Các thiết bị mạng quan trọng như tường lửa (firewall), thiết bị định tuyến (router), hệ thống máy chủ, … 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. Phòng máy chủ là khu vực hạn chế tiếp cận, chỉ cán bộ chuyên trách CNTT và người được phép vào phòng máy chủ.

4. Giám sát, nhắc nhở, khuyến cáo CBCC thay đổi mật khẩu thường xuyên.

5. Tổ chức hướng dẫn, tập huấn về phòng chống mã độc, các rủi ro do mã độc gây ra cho CBCC trong toàn cơ quan.

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

7. 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.

8. Triển khai các giải pháp tổng thể bảo đảm an toàn, an ninh thông tin mạng trong toàn hệ thống; các giải pháp kỹ thuật phòng chống virus, mã độc, thư rác cho hệ thống và máy tính cá nhân cho CBCC trong cơ quan.

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 CBCC 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 cán bộ chuyên trách CNTT của đơn vị để kịp thời ngăn chặn và xử lý.

4. Nâng cao ý thức cảnh giác và trách nhiệm về an toàn, an ninh thông tin. Tham gia đầy đủ 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 theo Điều 7, Thông tư số 04/2015/TT-TTCP ngày 09/7/2015 của Thanh tra Chính phủ quy định công tác bảo vệ bí mật nhà nước trong ngành Thanh tra.

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.

Điều 10. Trách nhiệm của các phòng thuộc Thanh tra tỉnh

1. Trưởng phòng có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước Chánh Thanh tra tỉnh trong công tác đảm bảo an toàn thông tin của phòng 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 cán bộ thường xuyên theo dõi để đảm bảo an toàn thông tin của 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.

Điều 11. Trách nhiệm của Trưởng đoàn và thành viên các Đoàn thanh tra, Đoàn tham mưu, giải quyết khiếu nại, tố cáo (KN,TC), phòng, chống tham nhũng

1. Chậm nhất sau 10 ngày làm việc khi Đoàn thanh tra đã xây dựng Báo cáo thanh tra, giải quyết KN,TC, phòng, chống tham nhũng, Trưởng đoàn có trách nhiệm phân công cán bộ tập hợp toàn bộ các văn bản, tài liệu điện tử hình thành trong quá trình hoạt động của các thành viên Đoàn thanh tra, Đoàn tham mưu, giải quyết KN,TC, để lưu vào USB copy vào máy tính để bàn không kết nối mạng. *(Lưu vào các thư mục theo hướng dẫn mẫu tại Phụ lục 02 kèm theo)*

Các thành viên Đoàn thanh tra, Đoàn tham mưu, giải quyết KN,TC có trách nhiệm xoá toàn bộ thông tin mà mình có được trong quá trình tham gia Đoàn thanh tra, giải quyết KN,TC.

Chậm nhất sau 5 ngày khi cấp có thẩm quyền ban hành Kết luận thanh tra, Quyết định giải quyết khiếu nại, Kết luận tố cáo, Trưởng đoàn có trách nhiệm copy vào USB theo hướng dẫn tại Phụ lục 02 và chuyển cho cán bộ chuyên trách CNTT cơ quan.

2. Chậm nhất sau 01 ngày khi nhận USB, cán bộ chuyên trách CNTT copy lưu dữ liệu vào thiết bị lưu trữ của cơ quan và chuyển trả USB cho Trưởng đoàn.

3. Nghiêm cấm các cá nhân lưu giữ các thông tin, tài liệu, thiết bị mang bí mật nhà nước hình thành trong quá trình tham gia các Đoàn thanh tra, tham mưu giải quyết khiếu nại, tố cáo.

4. USB được Văn phòng cung cấp cho mỗi phòng chỉ để dùng lưu dữ liệu các đoàn Thanh tra, giải quyết KN,TC và phòng chống tham nhũng.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 12. Khen thưởng và xử lý vi phạm

1. Các phòng thuộc Thanh tra tỉnh; CBCC thực hiện tốt Quy chế này sẽ được xem xét đánh giá khen thưởng.

2. Các phòng thuộc Thanh tra tỉnh; CBCC có hành vi vi phạm quy chế này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật theo quy định pháp luật 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 báo cáo về Văn phòng tổng hợp trình Lãnh đạo xem xét, giải quyết./.

CHÁNH THANH TRA