

Số: 43/QĐ-UBND

Hương Thủy, ngày 18 tháng 01 năm 2017

QUYẾT ĐỊNH

**Ban hành Quy định an toàn, an ninh thông tin
trên môi trường mạng trong hoạt động của các cơ quan nhà nước
trên địa bàn thị xã Hương Thủy**

ỦY BAN NHÂN DÂN THỊ XÃ

Căn cứ Luật Tổ chức Chính quyền địa phương 19 tháng 6 năm 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 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; Nghị định số 72/2013/NĐ-CP ngày 15/07/2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng;

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;

Theo đề nghị của Chánh Văn phòng HĐND và UBND thị xã Hương Thủy,

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 của các cơ quan, đơn vị quản lý Nhà nước trên địa bàn thị xã Hương Thủy.

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

Điều 3. Chánh Văn phòng Hội đồng nhân dân và Ủy ban nhân dân thị xã, Thủ trưởng các phòng, ban chuyên môn trực thuộc, Chủ tịch Ủy ban nhân dân các xã, phường; và các cơ quan, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:

- Như Điều 3;
- Sở Thông tin và Truyền thông;
- TT.HĐND thị xã;
- CT, các PCT.UBND thị xã;
- Lưu: VT.

TM. ỦY BAN NHÂN DÂN
KT.CHỦ TỊCH
PHÓ CHỦ TỊCH
(Đã ký)
Nguyễn Thanh Minh

QUY ĐỊNH

**Đảm bảo an toàn, an ninh thông tin trên môi trường mạng
trong hoạt động của các cơ quan nhà nước trên địa bàn thị xã Hương Thủy**
*(Ban hành kèm theo Quyết định số 43 /QĐ-UBND ngày 18/01/2017 của Ủy ban
nhân dân thị xã Hương Thủy)*

Chương I

QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy định về công tác đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của các cơ quan nhà nước trên địa bàn thị xã Hương Thủy.

Điều 2. Đối tượng áp dụng

1. Quy định này áp dụng đối với các cơ quan nhà nước thị xã Hương Thủy, bao gồm: các phòng, ban trực thuộc UBND thị xã; Ủy ban nhân dân các xã, phường (sau đây gọi tắt là các cơ quan, đơn vị).

3. Cán bộ, công chức, viên chức đang làm việc trong các cơ quan, đơn vị nêu tại khoản 1 Điều này và những tổ chức, cá nhân có liên quan áp dụng Quy định này trong việc đảm bảo an toàn thông tin tại các cơ quan, đơn vị.

Điều 3. Mục đích, nguyên tắc đảm bảo an toàn thông tin

1. Tăng cường khả năng phòng chống nguy cơ tấn công, xâm nhập hệ thống thông tin và ngăn chặn, khắc phục kịp thời các sự cố gây mất an toàn thông tin trên môi trường mạng.

2. Công tác đảm bảo an toàn, bảo mật thông tin trên môi trường mạng là yêu cầu bắt buộc trong quá trình thiết kế, vận hành, nâng cấp và huỷ bỏ hạ tầng kỹ thuật, hệ thống thông tin của cơ quan nhà nước.

3. Thông tin số được quy định danh mục bí mật nhà nước, văn bản điện tử có nội dung mật không được truyền đưa trên môi trường mạng và phải được phân loại, lưu trữ, bảo vệ theo quy định của pháp luật về bảo vệ bí mật nhà nước.

Điều 4. Giải thích từ ngữ

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

1. Hệ thống thông tin là tập hợp thiết bị phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin số.

2. An toàn thông tin là sự bảo vệ thông tin và các hệ thống thông tin tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

3. 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.

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

5. 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.

Chương II

NỘI DUNG ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 5. Trang thiết bị và hạ tầng công nghệ thông tin

1. 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 riêng biệt và có các biện pháp bảo vệ, ngăn chặn xâm nhập trái phép. Phòng máy phải có hệ thống lưu điện để đảm bảo duy trì hệ thống thiết bị hoạt động liên tục.

2. Máy chủ, máy tính cá nhân, thiết bị mạng, thiết bị tường lửa... của các cơ quan, đơn vị phải được bảo vệ bởi mật khẩu an toàn, có độ phức tạp cao và không sử dụng mật khẩu ngắn, mặc định. Cấp quyền truy cập các thiết bị phù hợp cho từng đối tượng.

3. Mạng riêng ảo (VPN) của đơn vị (nếu có) kết nối để truy cập vào hệ thống thông tin phải được bảo mật; quản lý và kiểm soát chặt chẽ các kết nối; hủy bỏ kết nối khi không còn sử dụng.

4. Lãnh đạo cơ quan, đơn vị phải chỉ đạo thực hiện chặt chẽ việc bảo vệ an toàn vật lý cho tất cả hệ thống công nghệ thông tin của cơ quan, đơn vị mình.

5. Tất cả các máy tính tại cơ quan, đơn vị phải được cài đặt phần mềm phòng chống vi rút, phần mềm độc hại. Không tải và cài đặt các phần mềm lạ, không rõ nguồn gốc. Thực hiện tắt máy tính khi không sử dụng trong thời gian dài hoặc hết thời gian làm việc để tránh các nguy cơ tấn công, xâm nhập trái phép.

6. Sử dụng các thiết bị lưu trữ gắn ngoài và thiết bị điện tử khác an toàn, đúng quy định.

7. Hệ thống thông tin của đơn vị phải có cơ chế sao lưu dữ liệu và thực hiện thường xuyên, định kỳ; thiết bị lưu trữ dữ liệu được sao lưu phải đảm bảo yêu cầu kỹ thuật; dữ liệu được sao lưu phải đảm bảo tính sẵn sàng và toàn vẹn, đáp

ứng yêu cầu phục hồi dữ liệu cho hệ thống thông tin hoạt động bình thường khi có sự cố xảy ra.

Điều 6. Quy định về quản trị, sử dụng các phần mềm và trao đổi thông tin trên môi trường mạng

1. Mỗi tài khoản truy cập các hệ thống phần mềm chỉ được cấp cho một người quản lý và sử dụng. Người sử dụng phải có trách nhiệm bảo mật tài khoản truy cập của mình.

2. Cán bộ, công chức, viên chức phải thay đổi mật khẩu mặc định khi đăng nhập lần đầu vào các Hệ thống phần mềm, Thư điện tử công vụ... Mật khẩu phải có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, gồm ký tự thường, ký tự hoa, ký tự số và ký tự đặc biệt như !, @, #, \$, %,...) và phải thường xuyên thay đổi nhằm tăng cường công tác bảo mật

3. Đối với cán bộ, công chức, viên chức đã nghỉ việc, chuyển công tác phải khóa tài khoản, hủy quyền truy cập, thu hồi các thiết bị liên quan tới hệ thống thông tin (khóa, thẻ nhận dạng, công cụ ký số,...) nhưng vẫn đảm bảo khả năng truy cập vào các hồ sơ được tạo ra bởi tài khoản đó.

4. Việc sử dụng, chia sẻ và lưu trữ dữ liệu, thông tin số trên mạng nội bộ, mạng Internet phải tuân thủ các quy định của cơ quan, đơn vị và quy định pháp luật về viễn thông, công nghệ thông tin; Khi thực hiện chia sẻ tài nguyên trên máy tính phải sử dụng mật khẩu để bảo vệ thông tin. Khuyến cáo người dùng cân nhắc việc chia sẻ tài nguyên cục bộ trên máy đang sử dụng, tuyệt đối không được chia sẻ toàn bộ ổ cứng.

5. Sử dụng chức năng mã hóa ở mức hệ điều hành khi cần thiết để bảo đảm các dữ liệu không bị thay đổi trước khi truyền trên môi trường mạng. Các tệp tin đính kèm thư điện tử hoặc được tải xuống từ mạng Internet hay từ các thiết bị lưu trữ ngoài khi thực hiện sao chép, kết nối với máy tính cần được kiểm tra để phòng chống vi rút, phần mềm độc hại.

6. Không cài đặt phần mềm không rõ nguồn gốc hoặc can thiệp tới các phần mềm ứng dụng khác trên hệ thống thông tin của cơ quan, đơn vị khi chưa được cấp có thẩm quyền cho phép.

7. Không sử dụng tên tài khoản thư điện tử công vụ trên các mạng xã hội, các diễn đàn và các trang thông tin khác trên mạng Internet. Sử dụng thư điện tử công vụ trong các hoạt động công vụ; tuân thủ các quy định về sử dụng thư điện tử công vụ.

Điều 7. Đối với cán bộ chuyên trách CNTT.

1. Được đảm bảo điều kiện về đào tạo, bồi dưỡng, học tập, nghiên cứu, tiếp thu kiến thức, kỹ thuật và công nghệ mới đối với lĩnh vực an toàn, an ninh thông tin.

2. Tham mưu về chuyên môn và vận hành an toàn hệ thống thông tin của đơn vị; triển khai các giải pháp kỹ thuật phòng chống virus, mã độc hại, thư rác cho hệ thống và máy tính cá nhân; kiểm soát và có giải pháp kỹ thuật chống truy cập trái phép vào hệ thống thông tin. Triển khai các biện pháp bảo đảm an toàn thông tin cho cán bộ, công chức, viên chức trên địa bàn;

3. Quản lý chặt chẽ việc di chuyển các trang thiết bị công nghệ thông tin lưu trữ các thông tin thuộc danh mục bí mật nhà nước.

4. Thực hiện cấp phát, thu hồi, cập nhật và quản lý tất cả các tài khoản truy cập vào hệ thống thông tin của đơn vị; hướng dẫn người sử dụng thay đổi mật khẩu ngay sau khi đăng nhập lần đầu tiên; bảo vệ thông tin của tài khoản theo quy định.

5. Thường xuyên thực hiện phân tích, đánh giá và báo cáo các rủi ro và nguy cơ gây mất an toàn, an ninh thông tin đối với hệ thống thông tin của đơn vị; nguyên nhân gây ra các rủi ro và nguy cơ gây mất an toàn, an ninh thông tin mạng bao gồm: Hiện tượng tự nhiên (nhiệt độ, không khí, mưa bão, sét), truy cập trái phép, virus, cố ý làm thay đổi thông số cấu hình hệ thống và phá hủy dữ liệu. Đồng thời tham mưu và xây dựng phương án hạn chế, khắc phục các rủi ro và nguy cơ có thể xảy ra.

6. Phối hợp với các cá nhân, đơn vị liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn, an ninh thông tin. Kiểm soát chặt chẽ cài đặt phần mềm trên máy chủ, máy trạm.

Điều 8. Bảo vệ bí mật nhà nước trong hoạt động ứng dụng công nghệ thông tin

1. Quy định về soạn thảo, in ấn, phát hành và sao chụp tài liệu mật:

a) Không được sử dụng máy tính nối mạng internet 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 Trang thông tin điện tử.

b) Không được in, sao chụp tài liệu bí mật nhà nước trên các thiết bị kết nối mạng internet.

2. Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật không được cho phép các công ty tư nhân hoặc người không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố.

3. Trước khi thanh lý các máy tính trong các cơ quan nhà nước, cán bộ chuyên trách công nghệ thông tin phải dùng các biện pháp kỹ thuật xóa bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

Điều 9. Giải quyết và khắc phục sự cố an toàn, an ninh thông tin

1. Đối với người sử dụng:

a) Thông tin, báo cáo kịp thời cho cán bộ chuyên trách về công nghệ thông tin của cơ quan khi phát hiện các sự cố gây mất an toàn, an ninh thông tin mạng trong quá trình tham gia vào hệ thống thông tin của đơn vị.

b) Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

2. Đối với cán bộ chuyên trách về công nghệ thông tin:

a) Xử lý khẩn cấp: Khi phát hiện hệ thống nội bộ bị tấn công, thông qua các dấu hiệu như luồng tin (traffic) tăng lên bất ngờ, nội dung bị thay đổi, hệ thống hoạt động chậm bất thường cần kịp thời áp dụng mọi biện pháp để khắc phục và hạn chế mức thấp nhất thiệt hại có thể xảy ra.

Lập biên bản ghi nhận sự cố gây ra mất an toàn, an ninh thông tin đối với hệ thống thông tin của cơ quan, đơn vị; đồng thời thu thập các chứng cứ, dấu vết và nguyên nhân gây ra sự cố (nếu có); đồng thời báo cáo sự cố và kết quả khắc phục sự cố cho Thủ trưởng cơ quan, đơn vị.

b) Trường hợp phát hiện sự cố xảy ra nghiêm trọng ngoài khả năng giải quyết của đơn vị, phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông để được hỗ trợ, hướng dẫn và phối hợp khắc phục sự cố; đồng thời tham mưu văn bản báo cáo sự cố gửi Sở Thông tin và Truyền thông và các đơn vị có liên quan.

Chương III

TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 10. Trách nhiệm của các cơ quan, đơn vị

1. Thủ trưởng các cơ quan, đơn vị có trách nhiệm tổ chức thực hiện các nội dung trong Quy định này và chịu trách nhiệm trước Ủy ban nhân dân thị xã trong công tác đảm bảo an toàn thông tin của cơ quan, đơn vị mình.

2. Thực hiện và chỉ đạo cán bộ, công chức thuộc thẩm quyền quản lý thực hiện nghiêm túc Quy định này.

3. Tạo điều kiện thuận lợi cho cán bộ, công chức được đào tạo, bồi dưỡng kỹ năng an toàn, an ninh thông tin mạng.

4. Quan tâm đầu tư các thiết bị phần cứng, phần mềm liên quan đến công tác đảm bảo an toàn, an ninh thông tin.

5. Tạo điều kiện thuận lợi cho các cơ quan chức năng trong công tác điều tra, làm rõ nguyên nhân gây ra sự cố; lực lượng kỹ thuật tham gia khắc phục sự cố và thực hiện đúng theo hướng dẫn.

Điều 11. Trách nhiệm của cán bộ, công chức, viên trong các cơ quan, đơn vị

1. Trách nhiệm của cán bộ, công chức, viên chức tham gia sử dụng và khai thác hệ thống thông tin:

a) Nghiêm chỉnh chấp hành các quy chế nội bộ, quy trình đảm bảo an toàn, an ninh thông tin của cơ quan, đơn vị, các nội dung của Quy định 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.

b) 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 công nghệ thông tin của đơn vị để kịp thời ngăn chặn, xử lý.

c) Nâng cao ý thức cảnh giác và trách nhiệm về an toàn, an ninh thông tin.

2. Trách nhiệm của cán bộ chuyên trách công nghệ thông tin:

a) Chịu trách nhiệm triển khai các biện pháp quản lý vận hành, quản lý kỹ thuật và tham mưu xây dựng các quy định về đảm bảo an toàn, an ninh thông tin mạng cho toàn bộ hệ thống thông tin của đơn vị mình đúng theo nội dung Quy định này.

b) Chủ động phối hợp với cá nhân, đơn vị có liên quan trong việc kiểm tra, phát hiện và khắc phục sự cố về an toàn, an ninh thông tin.

c) Tuân thủ theo sự hướng dẫn kỹ thuật của Sở Thông tin và Truyền thông trong quá trình khắc phục sự cố về an toàn, an ninh thông tin.

Chương IV

TỔ CHỨC THỰC HIỆN

Điều 12. Tổ chức thực hiện

Văn phòng HĐND và UBND thị xã chủ trì, phối hợp với các phòng, ban liên quan và UBND các xã, phường triển khai thực hiện nội dung của quy định này.

Trong quá trình thực hiện Quy định này, nếu có vướng mắc đề nghị các cơ quan, đơn vị gửi văn bản về UBND thị xã (qua Văn phòng HĐND và UBND thị xã) để xem xét, sửa đổi, bổ sung cho phù hợp./.

TM. ỦY BAN NHÂN DÂN
KT.CHỦ TỊCH
PHÓ CHỦ TỊCH

Nguyễn Thanh Minh