

Số: /QĐ-UBND

Thừa Thiên Huế, ngày tháng năm 2016

Dự thảo

QUYẾT ĐỊNH

Ban hành Quy định Bảo mật thông tin cá nhân của người dân, tổ chức và doanh nghiệp khi tham gia vào hệ thống dịch vụ công và cơ sở dữ liệu công dân, doanh nghiệp do các cơ quan nhà nước tỉnh Thừa Thiên Huế triển khai.

ỦY BAN NHÂN DÂN TỈNH

Căn cứ Luật Tổ chức Hội đồng nhân dân và Ủy ban nhân dân ngày 26 tháng 11 năm 2003;

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

Căn cứ Thông tư số 25/2010/TT-BTTTT ngày 15 tháng 11 năm 2010 của Bộ Thông tin và Truyền thông quy định việc thu thập, sử dụng, chia sẻ, đảm bảo an toàn và bảo vệ thông tin cá nhân trên trang thông tin điện tử hoặc cổng thông tin điện tử của cơ quan nhà nước;

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

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số/TTr-STTTT ngày tháng năm 2015,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế Bảo mật thông tin cá nhân của người dân, tổ chức, doanh nghiệp khi tham gia vào hệ thống thông tin của cơ quan nhà nước trên địa bàn tỉnh Thừa Thiên Huế.

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

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh; Giám đốc Sở Thông tin và Truyền thông; Thủ trưởng các Sở, ban, ngành; Chủ tịch Ủy ban nhân dân các huyện, thị xã, thành phố Huế; Các đơn vị sự nghiệp thuộc tỉnh; Các cơ quan, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:

- Như Điều 3;
- Bộ Thông tin và Truyền thông;
- TT TU, TT HĐND;
- CT, các PCT UBND tỉnh;
- Ban Nội chính Tỉnh ủy;
- Công an tỉnh;
- Công TTĐT tỉnh;
- VP: CVP, PCVP Đ.N.Trân;
- Lưu: VT, DL.

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

Phan Ngọc Thọ

QUY ĐỊNH

Ban hành Quy định Bảo mật thông tin cá nhân của người dân, tổ chức và doanh nghiệp khi tham gia vào hệ thống dịch vụ công và cơ sở dữ liệu công dân, doanh nghiệp do các cơ quan nhà nước tỉnh Thừa Thiên Huế triển khai.

*(Ban hành kèm theo Quyết định số /QĐ-UBND ngày
của UBND tỉnh Thừa Thiên Huế)*

Chương I QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Văn bản này quy định việc thu thập, sử dụng, chia sẻ, đảm bảo an toàn và bảo vệ thông tin cá nhân của người dân, tổ chức và doanh nghiệp khi tham gia vào hệ thống dịch vụ công, hệ thống phần mềm và cơ sở dữ liệu công dân, doanh nghiệp do các cơ quan nhà nước tỉnh Thừa Thiên Huế triển khai. (sau đây gọi tắt là hệ thống thông tin). Cụ thể, hệ thống thông tin trong các cơ quan nhà nước của tỉnh có thể là công/ trang thông tin điện tử, hệ thống thông tin kinh tế xã hội của tỉnh hay hệ thống cung cấp dịch vụ công trực tuyến các ngành và các hệ thống thông tin khác được đầu tư từ ngân sách nhà nước.

Điều 2. Đối tượng áp dụng

1. Quy định này được áp dụng đối với các cơ quan nhà nước trên địa bàn tỉnh Thừa Thiên Huế có triển khai các hệ thống thông tin, bao gồm: Các cơ quan chuyên môn thuộc Ủy ban nhân dân tỉnh và các đơn vị sự nghiệp trực thuộc; Các đơn vị sự nghiệp trực thuộc Ủy ban nhân dân tỉnh; Ủy ban nhân dân cấp huyện; Ủy ban nhân dân cấp xã (sau đây gọi tắt là cơ quan, đơn vị).

2. Cán bộ, công chức, viên chức đang làm việc trong các cơ quan, đơn vị nêu tại Khoản 1 Điều này và người dân, tổ chức, doanh nghiệp (sau đây gọi tắt là Người sử dụng) có liên quan áp dụng Quy định này trong việc vận hành, khai thác hệ thống thông tin tại các cơ quan, đơn vị.

Điều 3. Mục đích, nguyên tắc bảo mật thông tin cá nhân của người sử dụng

1. Việc áp dụng Quy chế này nhằm tránh được các nguy cơ thông tin cá nhân của người sử dụng bị phát tán hay bị sử dụng không đúng mục đích mà không được sự cho phép của người sử dụng khi tham gia các hệ thống thông tin của các cơ quan, đơn vị.

2. Công tác bảo mật thông tin của người sử dụng khi tham gia vào hệ thống thông tin của cơ quan, đơn vị là nhiệm vụ nhằm góp phần thúc đẩy quá trình xây dựng chính phủ điện tử phát triển hiệu quả; củng cố và tăng cường uy tín của các cơ quan nhà nước trên địa bàn tỉnh.

3. Các hệ thống thông tin của các cơ quan đơn, vị phải được xây dựng và vận hành tuân theo nguyên tắc đảm bảo an toàn thông tin được quy định tại Điều 41, Nghị định 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước.

4. Việc thu thập, sử dụng và chia sẻ thông tin cá nhân qua hệ thống thông tin của các cơ quan, đơn vị phải được sự đồng ý của cá nhân đó trừ những trường hợp pháp luật có quy định khác và được bảo vệ và đảm bảo an toàn.

5. Việc trao đổi, truyền đưa, lưu trữ thông tin cá nhân trên các hệ thống thông tin của các cơ quan, đơn vị được bảo vệ và đảm bảo an toàn theo quy định pháp luật.

Điều 4. Giải thích từ ngữ

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

Thông tin cá nhân là thông tin đủ để xác định chính xác danh tính một cá nhân, bao gồm ít nhất một trong những thông tin sau đây: họ tên, ngày sinh, nghề nghiệp, chức danh, địa chỉ liên hệ, địa chỉ thư điện tử, số điện thoại, số chứng minh nhân dân, số hộ chiếu. Những thông tin thuộc bí mật cá nhân gồm có hồ sơ y tế, hồ sơ nộp thuế, số thẻ bảo hiểm xã hội, số thẻ tín dụng và những bí mật cá nhân khác.

Chương II

NHỮNG QUY ĐỊNH VỀ BẢO MẬT THÔNG TIN CÁ NHÂN

Điều 5. Thu thập và sử dụng thông tin cá nhân

1. Cơ quan, đơn vị thông báo và hướng dẫn cho cá nhân biết về hình thức, phạm vi và mục đích của việc thu thập và sử dụng thông tin cá nhân.

2. Hình thức thu thập thông tin cá nhân bao gồm: người sử dụng điền thông tin vào phiếu đăng ký trực tiếp hoặc qua mạng, thông tin được tự động thu thập trong quá trình người sử dụng tham gia vào hệ thống thông tin.

3. Cơ quan, đơn vị chỉ yêu cầu những thông tin cá nhân thiết yếu theo Khoản 1, Điều 4 tại Quy định này phục vụ cho việc trao đổi thông tin giữa người sử dụng và cơ quan, đơn vị trong quá trình giao dịch và sử dụng thông tin cá nhân cho những mục đích đã được nêu rõ trước khi tiến hành thu thập thông tin.

Điều 6. Truy cập và cập nhật thông tin cá nhân

1. Ứng với mỗi hệ thống thông tin, cơ quan, đơn vị phải cung cấp cho người sử dụng quyền truy cập vào thông tin cá nhân của mình thông qua tài khoản sử dụng hệ thống; người sử dụng cập nhật thông tin về tài khoản của mình và cập nhật mật khẩu với độ dài và phức tạp hợp lý để đảm bảo bảo mật tài khoản. Cụ thể mật khẩu phải dài trên ký tự bao gồm chữ hoa, chữ thường, chữ số và ký hiệu đặc biệt. Người sử dụng tự bảo vệ mật khẩu cho tài khoản của mình, không được cung cấp mật khẩu hoặc để lộ mật khẩu cho người khác.

2. Trường hợp cá nhân không thể đăng nhập để xem thông tin của mình thì có quyền đề nghị cơ quan, đơn vị liên quan cấp lại thông tin về tài khoản và mật khẩu đăng nhập hoặc đề nghị kiểm tra chính, bổ sung, sửa đổi thông tin cá nhân; cơ quan, đơn vị tiếp nhận thông tin cá nhân cần cập nhật kịp thời, nhanh chóng.

Điều 7. Cung cấp, chia sẻ thông tin cá nhân

1. Các cơ quan, đơn vị không được cung cấp, chia sẻ thông tin cá nhân của người sử dụng cho bất kỳ tổ chức, cá nhân nào trừ khi người sử dụng đồng ý hoặc cơ quan, đơn vị có thẩm quyền yêu cầu hoặc pháp luật có quy định khác.

2. Cơ quan, đơn vị khi tiếp nhận thông tin cá nhân từ một cơ quan nhà nước khác theo quy định pháp luật phải có trách nhiệm đảm bảo an toàn và sử dụng thông tin cá nhân đúng mục đích.

Điều 8. Các hoạt động cơ bản nhằm bảo mật thông tin cá nhân

Các cơ quan, đơn vị khi triển khai hệ thống thông tin, nhằm bảo mật thông tin cá nhân của người sử dụng khi tham gia vào hệ thống phải có trách nhiệm thực hiện các việc sau:

1. Xây dựng, ban hành và công khai quy định hoặc công khai việc tuân theo quy định sẵn có liên quan đến bảo mật thông tin cá nhân khi sử dụng hệ thống; đồng thời hướng dẫn và kiểm tra thường xuyên việc thực hiện quy định.

2. Thực hiện các biện pháp kỹ thuật để đảm bảo bảo mật thông tin cá nhân; chống truy cập, sử dụng, thay đổi, phát tán trái phép thông tin cá nhân và các hành vi không được phép khác.

- Trang bị cơ sở hạ tầng kỹ thuật theo tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin cá nhân.

- Sử dụng công nghệ mã hóa đối với thông tin thuộc bí mật cá nhân.

- Áp dụng các thao tác kỹ thuật về quản lý an toàn hạ tầng kỹ thuật, chẳng hạn: Thiết lập hệ thống tường lửa; Mã hóa tín hiệu trên đường truyền; Sử dụng tài khoản, mật khẩu với độ phức tạp hợp lý; Xây dựng biện pháp dự phòng để giảm thiểu tác động xấu khi xảy ra mất an toàn đối với thông tin cá nhân.

Điều 9. Lưu giữ thông tin cá nhân

1. Đối với thông tin cá nhân của người sử dụng khi tham gia dịch vụ công trực tuyến, cơ quan, đơn vị có trách nhiệm lưu trữ thông tin này trên hệ thống thông tin tới khi nào còn cần thiết để thực hiện dịch vụ công trực tuyến được đăng ký.

2. Đối với người sử dụng tham gia các hệ thống thông tin nhiều lần hoặc mang tính định kỳ, lâu dài, các cơ quan, đơn vị có trách nhiệm lưu giữ thông tin cá nhân này trên máy tính trong thời gian mà hệ thống thông tin còn hoạt động.

3. Thông tin cá nhân được thu thập để phục vụ cho mục đích khảo sát, thống kê chỉ được lưu trữ đến khi công tác khảo sát, thống kê kết thúc.

Điều 10. Kiểm tra, đánh giá mức độ bảo mật thông tin cá nhân

1. Cơ quan chủ quản cần tiến hành kiểm tra, đánh giá thường xuyên về mức độ đảm bảo sự bảo mật của thông tin cá nhân.

2. Quy trình kiểm tra, đánh giá phải đáp ứng các yêu cầu sau đây:

a) Tuân thủ các quy định pháp luật;

b) Xác định nội dung thu thập, mục đích thu thập, mục đích sử dụng, các cơ quan được chia sẻ thông tin cá nhân;

c) Đánh giá hiệu quả và rủi ro của việc thu thập, sử dụng và chia sẻ thông tin cá nhân;

d) Kiểm tra và đánh giá mức độ đảm bảo an toàn và bảo vệ thông tin cá nhân;

đ) Kiểm định hạ tầng kỹ thuật về mặt an toàn thông tin phù hợp với các tiêu chuẩn, quy chuẩn kỹ thuật được quy định;

e) Xây dựng biện pháp dự phòng để giảm thiểu tác động xấu khi xảy ra mất an toàn đối với thông tin cá nhân;

g) Nghiên cứu các hạn chế của hệ thống thông tin liên quan đến bảo đảm tính toàn vẹn của thông tin cá nhân để tiến hành các biện pháp khắc phục kịp thời.

3. Ngay khi có sự thay đổi hoặc nâng cấp hệ thống thông tin, cơ quan chủ quản phải kiểm tra đánh giá lại về mức độ đảm bảo sự bảo mật của thông tin cá nhân.

Điều 11. Điều kiện đảm bảo an toàn và bảo vệ thông tin cá nhân

1. Cán bộ, công chức trong cơ quan, đơn vị phải nắm vững các quy định pháp luật và nội quy của cơ quan về bảo đảm bảo mật thông tin cá nhân.

2. Cán bộ chuyên trách Công nghệ thông tin (CBCT CNTT) hoặc chuyên viên kỹ thuật phải được tuyển chọn, đào tạo, thường xuyên bồi dưỡng nghiệp vụ phù hợp với nhiệm vụ được giao và được tạo điều kiện làm việc phù hợp.

3. Ưu tiên sử dụng CBCT CNTT hoặc chuyên viên kỹ thuật của cơ quan, đơn vị để bảo đảm bảo mật thông tin cá nhân lưu trữ trên hệ thống thông tin. Trường hợp cần thiết có thể sử dụng dịch vụ đảm bảo an toàn thông tin của các tổ chức, doanh nghiệp bên ngoài nhưng phải có cam kết bằng văn bản với tổ chức, doanh nghiệp đó về đảm bảo bảo mật thông tin cá nhân.

4. Cơ quan, đơn vị có trách nhiệm bố trí kinh phí để phục vụ cho công tác đảm bảo bảo mật thông tin cá nhân trên hệ thống thông tin.

5. Đối với thông tin cá nhân được đăng ký trực tiếp, cơ quan, đơn vị cần bố trí con người và dụng cụ để lưu trữ hợp lý theo quy định của Nhà nước về Lưu trữ.

Điều 12. Các hành vi bị nghiêm cấm

1. Tự ý xâm nhập, sửa đổi, xóa bỏ nội dung thông tin cá nhân của người sử dụng đã được đăng ký.

2. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin cá nhân của người sử dụng khác trên môi trường mạng.

3. Các hành vi khác làm mất sự bảo mật thông tin cá nhân như cung cấp thông tin cá nhân của người sử dụng cho bên thứ ba mà không được sự đồng ý của người sử dụng hay không có quy định của pháp luật.

4. Sử dụng thông tin cá nhân của người sử dụng không đúng mục đích đã quy định.

Chương III

TRÁCH NHIỆM BẢO MẬT THÔNG TIN CÁ NHÂN

Điều 13. Trách nhiệm của các cơ quan, đơn vị

1. Thủ trưởng các cơ quan, đơn vị có trách nhiệm tổ chức thực hiện Quy định này và chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong việc đảm bảo bảo mật thông tin cá nhân khi tham gia vào các hệ thống thông tin do chính cơ quan, đơn vị triển khai.

2. Các cơ quan, đơn vị khi triển khai các hệ thống thông tin, phối hợp các đơn vị liên quan lồng ghép tổ chức tập huấn cho người sử dụng cách bảo mật thông tin cá nhân khi tham gia vào các hệ thống thông tin này qua mạng.

3. Khi có sự cố hoặc nguy cơ mất bảo mật thông tin cá nhân phải chỉ đạo khắc phục sự cố kịp thời và hạn chế thấp nhất mức thiệt hại có thể xảy ra.

4. Tạo điều kiện thuận lợi cho các cơ quan chức năng trong công tác điều tra, làm rõ nguyên nhân gây mất bảo mật thông tin cá nhân và cách khắc phục.

Điều 14. Trách nhiệm của Sở Thông tin và Truyền thông

1. Chịu trách nhiệm đảm bảo kỹ thuật về công tác bảo mật thông tin cá nhân khi tham gia vào hệ thống thông tin được triển khai diện rộng tại các cơ quan nhà nước trên phạm vi toàn tỉnh.

2. Tham mưu Ủy ban nhân dân tỉnh trong công tác quản lý thông tin cá nhân nhằm đảm bảo bảo mật thông tin cá nhân khi tham gia vào hệ thống thông tin của các cơ quan nhà nước trong tỉnh.

3. Thực hiện nhiệm vụ cảnh báo về nguy cơ hoặc sự cố gây mất bảo mật thông tin cá nhân.

4. Phối hợp với các đơn vị có liên quan trong thực hiện nhiệm vụ đảm bảo bảo mật thông tin cá nhân.

5. Tổng hợp báo cáo và thông báo về tình hình bảo mật thông tin cá nhân cho Bộ Thông tin và Truyền thông, Ủy ban nhân dân tỉnh và các cơ quan, đơn vị có liên quan khi có yêu cầu.

6. Tổ chức thực hiện việc tiếp nhận và xử lý các sự cố có nguy cơ làm mất an toàn bảo mật thông tin cá nhân.

Điều 15. Trách nhiệm của cán bộ, công chức, viên chức tại các cơ quan, đơn vị

1. 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.

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

a) Nghiêm túc thực hiện các nội quy, quy chế, quy định về đảm bảo bảo mật thông tin cá nhân khi tham gia vào hệ thống thông tin của cơ quan, đơn vị.

b) Khi phát hiện nguy cơ hoặc sự cố mất an toàn, an ninh thông tin mạng phải báo cáo kịp thời cho cán bộ chuyên trách công nghệ thông tin của đơn vị mình để kịp thời ngăn chặn và xử lý.

c) Nâng cao ý thức cảnh giác và trách nhiệm về bảo mật thông tin cá nhân.

Điều 16. Trách nhiệm của người sử dụng nói chung

1. Cung cấp thông tin cá nhân chính xác, đầy đủ, trung thực khi giao dịch trực tiếp cũng như trực tuyến qua hệ thống thông tin với cơ quan, đơn vị hoặc khi được cơ quan, đơn vị yêu cầu và chịu trách nhiệm đối với những thông tin cá nhân do mình cung cấp.

2. Giữ kín tài khoản cá nhân khi tham gia khai thác, sử dụng hệ thống thông tin của cơ quan, đơn vị và hoàn toàn chịu trách nhiệm đối với tất cả các hoạt động diễn ra thông qua việc sử dụng tài khoản của mình.

3. Tuân thủ các quy định và hướng dẫn của cơ quan, đơn vị để đảm bảo bảo mật thông tin cá nhân trên hệ thống thông tin của cơ quan, đơn vị này.

Chương IV

TỔ CHỨC THỰC HIỆN

Điều 17. Tổ chức thực hiện

1. Sở Thông tin và Truyền thông chủ trì, phối hợp với các cơ quan, đơn vị có liên quan triển khai thực hiện tốt nội dung Quy định này.

2. Thủ trưởng các cơ quan, đơn vị tổ chức triển khai thực hiện nghiêm túc Quy định này. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, phát sinh cần sửa đổi, bổ sung, đề nghị các cơ quan, đơn vị kịp thời báo cáo về Sở Thông tin và Truyền thông để tổng hợp trình Ủy ban nhân dân tỉnh xem xét, quyết định./.

ỦY BAN NHÂN DÂN TỈNH THỪA THIÊN HUẾ