UBND TỈNH QUẢNG TRỊ
BAN DÂN TỘC

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

Số: 128/QĐ-BDT

Quảng Trị, ngày 22 tháng 9 năm 2016

QUYẾT ĐỊNH

Ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin tại Ban Dân tộc tỉnh Quảng Trị

TRƯỞNG BAN DÂN TỘC TỈNH QUẢNG TRỊ

Căn cứ Quyết định số 35/2016/QĐ-UBND ngày 29/8/2016 của Ủy ban nhân dân tỉnh Quảng Trị về việc ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Quảng Trị;

Căn cứ Quyết định số 06/2015/QĐ-UBND ngày 24/4/2015 của UBND tỉnh Quảng Trị V/v ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Ban Dân tộc;

Xét đề nghị của Chánh Văn phòng Ban Dân tộc,

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 tại Ban Dân tộc tỉnh Quảng Trị.

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

Chánh Văn phòng, Trưởng các Phòng thuộc Ban và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 2;
- Sở Thông tin và Truyền thông;
- Trưởng, Phó Ban;
- Trang thông tin điện tử BDT;
- LưuVT,VP.

TRƯỞNG BAN

CỘNG HOÀ X.H.C.N VIỆT NAM
BAN DÂN TỘC
TỈNH QUẢNG TRỊ

Lê Văn Quyền

UBND TỈNH QUẢNG TRỊ
BAN DÂN TỘC

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 CNTT tại Ban Dân tộc tỉnh Quảng Trị

(Ban hành kèm theo Quyết định số 128/QĐ-BDT ngày 22/9/2016 của Ban Dân tộc)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Đối tượng áp dụng

Quy chế này được áp dụng đối với các Phòng và công chức thuộc Ban Dân tộc tỉnh Quảng Trị, các tổ chức, cá nhân và bên thứ 3 liên quan đến hoạt động quản lý, vận hành, khai thác hạ tầng, phần mềm công nghệ thông tin (CNTT) và đảm bảo an toàn, an ninh thông tin (AT-ANTT) trong ứng dụng CNTT.

Điều 2. Phạm vi điều chỉnh

Quy chế này quy định về công tác đảm bảo AT-ANTT trong hoạt động ứng dụng CNTT tại Ban Dân tộc tỉnh Quảng Trị.

Điều 3. Mục tiêu

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 hoạt động ứng dụng CNTT tại tại Ban Dân tộc tỉnh Quảng Trị.

Chương II
NỘI DUNG ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 4. Về quản lý kỹ thuật cơ bản cho công tác an toàn thông tin

1) Công chức có trách nhiệm quản lý trang thiết bị CNTT (máy vi tính, máy in, thiết bị ngoại vi,...) được giao sử dụng, tự quản lý dữ liệu trên máy tính của cá nhân, tự quyết định việc chia sẻ tài nguyên với các máy tính khác theo đúng quy chế. Đối với cơ sở dữ liệu thuộc dạng tài liệu "mật" theo quy chế khi chia sẻ, cung cấp phải có ý kiến của lãnh đạo Ban và được lưu trữ theo quy chế.

2) Công chức phụ trách CNTT của Ban chịu trách nhiệm kiểm tra, theo dõi, đánh giá sự hoạt động của hệ thống máy tính, các thiết bị mạng và các thiết bị ngoại vi theo đúng tiêu chuẩn kỹ thuật; thực hiện việc sao lưu dữ liệu thường xuyên; các thiết bị CNTT phải thực hiện công tác bảo trì, bảo dưỡng định kỳ, đột xuất, giảm thiểu tối đa các sự cố kỹ thuật.

Điều 5. Về quản lý vận hành trong công tác an toàn thông tin

1) Máy tính và các thiết bị CNTT để nơi an toàn, tránh ảnh hưởng của các tác nhân bên ngoài; không để các tài liệu, vật liệu dễ cháy gần máy tính và các thiết bị

CNTT để tránh xảy ra cháy nổ; thường xuyên vệ sinh cho máy vi tính; hàng ngày kiểm tra theo dõi sự hoạt động của máy vi tính và các thiết bị... Khi không sử dụng, phải tắt máy vi tính và các thiết bị để tiết kiệm điện và phòng, chống các xâm nhập trái phép.

2) Máy vi tính chứa dữ liệu quan trọng và thường xuyên kết nối Internet phải cài đặt các phần mềm diệt virus có bản quyền; có cơ chế bảo vệ thư mục và tập tin khi chia sẻ tài nguyên dùng chung.

3) Trong quá trình sử dụng các thiết bị CNTT, khi có sự cố xảy ra đối với các thiết bị CNTT, người sử dụng thiết bị CNTT thông báo với công chức phụ trách CNTT của cơ quan; nếu sự cố nhỏ, không phải thay thế hoặc sửa chữa linh kiện thì công chức phụ trách CNTT xử lý trực tiếp. Nếu có sự cố lớn, cần phải thay thế linh kiện để sửa chữa thì người dùng thiết bị CNTT phải làm đề xuất, có xác nhận của lãnh đạo Phòng (bộ phận) và gửi về Văn phòng Ban để được hướng dẫn sửa chữa, thay thế; tuyệt đối không được chuyển cho tập thể, cá nhân chưa được cơ quan xác nhận tính an toàn, bảo mật thông tin khi sửa chữa.

4) Hệ thống mạng không dây (wireless) của Ban phải được thiết lập khóa khi truy cập.

2. Hệ thống mạng LAN

a) Công chức khi tham gia vào mạng LAN không được tự ý thay đổi các tham số mạng, nếu tự ý thay đổi tham số mạng thì người thay đổi phải chịu hoàn toàn trách nhiệm. Trường hợp cần thiết phải thay đổi tham số mạng, báo công chức phụ trách CNTT của cơ quan biết để xử lý.

b) Công chức phụ trách CNTT chịu trách nhiệm kiểm tra, theo dõi, đánh giá sự hoạt động của hệ thống máy tính, các thiết bị mạng và các thiết bị khác theo đúng tiêu chuẩn kỹ thuật; thực hiện công tác bảo trì, bảo dưỡng định kỳ, đột xuất, giảm tối đa các sự cố kỹ thuật; cung cấp địa chỉ IP mạng và tham số mạng cho người dùng kết nối vào mạng LAN của cơ quan.

c) Công chức phụ trách CNTT chịu trách nhiệm hướng dẫn, cài đặt hệ thống an ninh mạng theo đúng tiêu chuẩn an toàn bảo mật; thường xuyên kiểm tra, quét virus cho tất cả các máy tính, xử lý khắc phục kịp thời khi xảy ra sự cố, đảm bảo hệ thống mạng máy tính hoạt động ổn định, liên tục.

d) Hàng năm công chức phụ trách CNTT lập kế hoạch mua sắm các thiết bị CNTT để đảm bảo an toàn cho các máy tính và mạng máy tính của cơ quan.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 6. Trách nhiệm của Lãnh đạo Ban

1. Phân công công chức phụ trách CNTT đảm bảo, an toàn thông tin trước khi tiến hành các hoạt động quản lý, vận hành hệ thống thông tin.

2. Bố trí kinh phí trang cấp các thiết bị phần cứng, phần mềm liên quan đến công tác đảm bảo AT-ANTT.

3. Khi có sự cố hoặc nguy cơ mất AT-ANTT phải kịp thời chỉ đạo các Phòng và cán bộ phụ trách CNTT phối hợp chặt chẽ với các cơ quan, đơn vị phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm AT-ANTT.

4. Chỉ đạo tăng cường công tác đảm bảo AT-ANTT trong hoạt động ứng dụng CNTT và quan tâm đầu tư các thiết bị AT-ANTT, phần mềm diệt virus có bản quyền cho máy tính ở cơ quan.

5. Có trách nhiệm tổ chức triển khai thực hiện các quy định tại Quy chế này, tuyên truyền, nâng cao nhận thức cho công chức về các nguy cơ mất AT-ANTT.

6. Phối hợp chặt chẽ với cơ quan Công an trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động vi phạn AT-ANTT.

Điều 7. Trách nhiệm của Văn phòng Ban

1. Tham mưu Trưởng Ban về công tác đảm bảo AT-ANTT trong hoạt động ứng dụng CNTT.

2. Xây dựng kế hoạch công việc và kinh phí thực hiện công tác AT-ANTT trong hoạt động ứng dụng CNTT của Ban.

3. Thông báo cho các Phòng biết để có biện pháp phòng ngừa, ngăn chặn các nguy cơ mất AT-ANTT do virus, phần mềm gián điệp,... gây ra.

Điều 8. Trách nhiệm của Phòng chuyên môn

1. Tuyên truyền, nâng cao nhận thức cho công chức thuộc Phòng về các nguy cơ mất AT-ANTT; tổ chức triển khai thực hiện Quy chế này.

2. Xây dựng quy trình AT-ANTT cho hệ thống thông tin nhằm giảm thiểu các nguy cơ gây ra sự cố, tạo điều kiện cho việc khắc phục và truy vết trong trường hợp có sự cố xảy ra.

3. Khi có sự cố hoặc nguy cơ mất an toàn thông tin phải kịp thời thông báo cho công chức phụ trách CNTT của Ban.

4. Phối hợp với Đoàn kiểm tra để triển khai công tác kiểm tra khắc phục sự cố; đồng thời cung cấp đầy đủ các thông tin khi Đoàn kiểm tra yêu cầu.

5. Khi sửa chữa, nâng cấp, mua sắm các thiết bị ứng dụng CNTT phải đề xuất với Văn phòng để tổng hợp trình lãnh đạo Ban giải quyết.

Điều 9. Trách nhiệm của công chức phụ trách CNTT

1. Xây dựng kế hoạch ứng dụng CNTT hàng năm của cơ quan.

2. Kịp thời tham mưu cho lãnh đạo Ban về quy chế, hướng dẫn có liên quan đến công tác đảm bảo AT-ANTT do cơ quan chuyên môn hướng dẫn.

3. Đảm bảo AT-ANTT đối với máy tính, hệ thống mạng của cơ quan.

4. Quản lý việc di chuyển các trang thiết bị CNTT như: máy tính, thiết bị ngoại

vi, hệ thống mạng..., thực hiện báo cáo kịp thời về tình trạng hoạt động an toàn hệ thống mạng, đề xuất hướng giải quyết khi có sự cố.

5. Thực hiện cấp phát, thu hồi, cập nhật và quản lý tất cả các tài khoản truy cập vào hệ thống thông tin của tỉnh; hướng dẫn người dùng thay đổi mật khẩu cá nhân theo quy chế.

6. Vận hành an toàn hệ thống thông tin của cơ quan, đơn vị, triển khai các biện pháp đảm bảo AT-ANTT cho tất cả cán bộ, công chức trong Ban .

7. Quản lý, theo dõi các hoạt động thường xuyên và định kỳ như vận hành, sửa chữa hệ thống máy vi tính, các thiết bị khác... Xử lý các yêu cầu về thay đổi tài khoản sử dụng mạng của các cơ quan .

Điều 10. Đối với công chức thuộc Ban

1. Công chức khi không sử dụng máy tính trong thời gian dài (quá 1 giờ làm việc) cần tắt máy, để tránh bị các hacker lợi dụng, sử dụng chức năng điều khiển từ xa tấn công vào hệ thống thông tin của cơ quan, đơn vị.

2. Công chức tự quản lý các thiết bị CNTT được giao sử dụng; không tự ý thay đổi và tháo lắp các thiết bị trên máy tính khi chưa có sự đồng ý của cán bộ phụ trách CNTT; không tự ý liên hệ với cá nhân bên ngoài vào can thiệp các thiết bị và mạng máy tính.

3. Sử dụng chức năng mã hóa đảm bảo các dữ liệu nhạy cảm như tài khoản, mật khẩu, các tập tin văn bản,... trước khi truyền trên môi trường mạng. Các tập tin gửi đính kèm bởi thư điện tử hoặc được tải xuống từ Internet hay các thiết bị lưu trữ gắn vào hệ thống cần được kiểm tra để phòng chống lây nhiễm virus hoặc phần mềm gián điệp làm mất thông tin.

4. Không được truy cập hoặc tải thông tin từ các Website độc hại, không được cài đặt các chương trình không rõ nguồn gốc...

5. Không sử dụng mạng xã hội như: Google Plus+, MySpace, LinkedIn, Twitter, Facebook, blog cá nhân tại cơ quan.

6. Không sử dụng hộp thư điện tử miễn phí Gmail, Yahoo mail trong hoạt động công vụ và tại máy tính có nối mạng ở cơ quan nhằm bảo đảm bảo mật, an toàn thông tin trên môi trường mạng.

7. Công chức sử dụng các thiết bị lưu trữ dữ liệu di động (máy tính xáy tay, thiết bị số cầm tay, thẻ nhớ USB, ổ cứng di động, băng từ..) để lưu thông tin thuộc danh mục bí mật nhà nước có trách nhiệm bảo vệ các thiết bị và thông tin trên thiết bị, tránh làm mất, lộ thông tin. Nghiêm cấm việc bán, cho mượn, giao người không có trách nhiệm sử dụng thiết bị do cá nhân tự trang bị có lưu trữ bí mật nhà nước.

8. Chấp hành các quy định nội bộ về an toàn thông tin của cơ quan và các quy định khác của pháp luật; nâng cao ý thức cảnh giác và trách nhiệm đảm bảo an ninh thông tin tại cơ quan.

Điều 11. Đối với người sử dụng

Nghiêm chỉnh chấp hành các quy chế nội bộ về AT-ANTT của cơ quan và các quy chế khác của pháp luật; nâng cao ý thức cảnh giác và trách nhiệm, đảm bảo AT-ANTT tại cơ quan.

Chương IV
QUY ĐỊNH VỀ QUẢN LÝ CÁC TÀI KHOẢN TRUY CẬP VÀO TỪNG HỆ THỐNG THÔNG TIN

Điều 12. Quy định quản lý tài khoản công chức

1. Công chức phụ trách CNTT có trách nhiệm phối hợp với Trung tâm tin học tỉnh trong việc cấp phát, thu hồi, cập nhật và quản lý các tài khoản truy nhập trên hệ thống thông tin của tỉnh dành cho cán bộ, công chức (CBCC) của Ban; tạo mới hoặc hủy bỏ tài khoản của công chức theo Quyết định điều động, bổ nhiệm, luân chuyển, nghỉ công tác,…. tại Ban.

2. Công chức phải có trách nhiệm bảo vệ và bảo mật tài khoản, dữ liệu của cá nhân, của Phòng và của cơ quan; không tự ý xâm nhập các tài khoản của người khác để sử dụng; không cung cấp thông tin tài khoản của cá nhân, cơ quan cho các tổ chức, cá nhân không có liên quan.

3. Mật khẩu phải thay đổi thường xuyên, tối thiểu mỗi quý 01 lần; không dùng một mật khẩu trong nhiều tài khoản.

Chương IV

QUY ĐỊNH VỀ CÔNG TÁC BẢO VỆ BÍ MẬT NHÀ NƯỚC VỀ AN TOÀN THÔNG TRIN TRÊN MÔI TRƯỜNG MẠNG

Điều 13. Bảo vệ bí mật nhà nước trong công tác ứng dụng công nghệ thông tin

1. Không được sử dụng thiết bị (máy tính để bàn, máy tính xách tay, máy tính bảng, điện thoại thông minh …) có kết nối mạng để soạn thảo văn bản, lưu trữ thông tin có nội dung thuộc bí mật nhà nước; không cung cấp tin, tài liệu và đưa thông tin bí mật nhà nước trên mạng.

2. Không bật các thiết bị kết nối mạng trong các cuộc họp có nội dung bí mật nhà nước.

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

4. Khi sửa chữa, khắc phục các sự cố của máy tính dùng để soạn thảo văn bản mật phải có sự giám sát, quản lý chặt chẽ của cán bộ có thẩm quyền.

5. Đối với các thiết bị CNTT, viễn thông, … được sử dụng để lưu trữ và truyền thông tin bí mật nhà nước phải được kiểm định của cơ quan chức năng trước khi đưa vào sử dụng.

6. Có biện pháp quản lý chặt chẽ trong việc sử dụng và thanh lý tài sản các trang thiết bị CNTT lưu trữ các thông tin thuộc danh mục bí mật nhà nước. Các

thiết bị lưu trữ không sử dụng cho công việc của cơ quan, đơn vị (thanh lý, cho, tặng) phải được xóa nội dung bằng phần mềm hoặc bằng thiết bị hủy dữ liệu chuyên dụng, đảm bảo không phục hồi được dữ liệu.

Chương IV
CƠ CHẾ SAO LƯU DỮ LIỆU

Điều 14. Cơ chế sao lưu dữ liệu

1. Định kỳ ít nhất 6 tháng một lần, các Phòng thuộc Ban phải tiến hành tổ chức lưu trữ, sao chép dữ liệu ra bộ nhớ ngoài như: ổ cứng gắn ngoài, đĩa CD, USB... (dữ liệu trong các máy tính phải tiến hành sao chép để bảo vệ là những dữ liệu chuyên môn phục vụ công tác của cơ quan).

2. Các Phòng thuộc Ban phải bảo quản, lưu trữ dữ liệu một cách an toàn và bảo mật. Các dữ liệu có tính chất quan trọng cần phải được mã hóa nhằm bảo vệ khỏi bị đánh cắp, lộ thông tin.

3. Không được lưu trữ, sao chép dữ liệu trên ổ đĩa cứng cài hệ điều hành.

Điều 15. Giải quyết và khắc phục sự cố về an toàn, an ninh thông tin

1. Đối với công chức

a) Thông báo kịp thời cho công chức phụ trách CNTT của Ban khi phát hiện các sự cố gây mất AT-ANTT trong hệ thống mạng.

b) Trường hợp xảy ra sự cố nghiêm trọng không khắc phục được phải kịp thời báo cáo cho cơ quan chuyên môn, cán bộ phụ trách CNTT (Phòng CNTT) của Sở Thông tin và Truyền thông tỉnh để có giải pháp xử lý kịp thời.

c) Xử lý khẩn cấp: Khi phát hiện hệ thống bị tấn công, thông qua các dấu hiệu khác thường như: Hệ thống máy tính hoạt động chậm khác thường, nội dung bị thay đổi,... cần thực hiện các bước sau:

- Ngắt kết nối máy vi tính ra khỏi mạng LAN, Internet.

- Sao chép toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ ngoài (USB, ổ cứng di động,...).

- Khôi phục hệ thống bằng cách chuyển dữ liệu backup (sao lưu) mới nhất để hệ thống hoạt động ổn định.

2. Đối với công chức phụ trách CNTT

a) Quản lý việc di chuyển các trang thiết bị CNTT của cơ quan.

b) Hướng dẫn người dùng các biện pháp kỹ thuật giải quyết và khắc phục sự cố; trong trường hợp sự cố xảy ra ngoài khả năng giải quyết, kịp thời báo cáo với lãnh đạo Ban; đồng thời phối hợp với cơ quan chuyên môn, cán bộ phụ trách CNTT của Sở Thông tin và Truyền thông để cùng phối hợp khắc phục.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 16. Công chức phụ trách CNTT

1. Trực tiếp tham mưu xử lý, khắc phục sự cố, hướng dẫn khắc phục sự cố về AT-ANTT của Ban.

2. Thường xuyên hướng dẫn công chức cơ quan khai thác và sử dụng tài nguyên CNTT và đảm bảo AT-ANTT.

Điều 17. Văn phòng Ban

1. Chủ trì, phối hợp với các Phòng thuộc Ban hướng dẫn việc thực hiện nghiêm túc Quy chế này và báo lãnh đạo Ban về AT-ANTT theo quy định.

2. Tổng hợp đề nghị bổ sung, chỉnh sửa quy chế; tham mưu đề xuất kinh phí mua các phần mềm, thiết bị và hạ tầng kỹ thuật để đảm bảo việc AT-ANTT.

Điều 18. Điều khoản thi hành

1. Các Phòng và cán bộ công chức thuộc Ban vi phạm quy chế này thì tùy theo tính chất, mức độ vi phạm sẽ bị xử lý kỷ luật theo trách nhiệm, xử phạt hành chính, bồi thường thiệt hại hoặc truy cứu trách nhiệm hình sự theo quy định hiện hành.

2. Trong quá trình thực hiện nếu có vấn đề phát sinh, chưa phù hợp cần sửa đổi, bổ sung các Phòng báo cáo bằng văn bản gửi Văn phòng để tổng hợp trình lãnh đạo Ban quyết định./.

TRƯỞNG BAN

CỘNG HÒA X.H.C.N VIỆT NAM
BAN DÂN TỘC
TỈNH QUẢNG TRỊ

Lê Văn Quyền