Ban Dân tộc
Ủy ban Nhân dân tỉnh Khánh Hòa
28.12.2018
13:58:52 +07:00

UBND TỈNH KHÁNH HÒA
BAN DÂN TỘC

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

Số: 105/QĐ-BDT

Khánh Hoà, ngày 28 tháng 12 năm 2018

QUYẾT ĐỊNH
Ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc

TRƯỞNG BAN DÂN TỘC TỈNH KHÁNH HÒA

Căn cứ Quyết định số 1786/QD-IJBND ngày 03/7/2015 cùa UBND tỉnh Khánh Hòa về việc kiện toàn chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Ban Dân tộc;

Căn cứ Quyết định số 38/2015/QĐ-UBND ngày 24/12/2015 của UBND tỉnh Khánh Hòa ban hành Quy định đảm bảo an toàn thông tin số trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Khánh Hòa;

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 thông tin trong hoạt động trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc.

Điều 2. Quyết định này có hiệu lực kể từ ngày ký và thay thế Quyết định số 55/QĐ-BDT ngày 19/10/2016 của Trưởng Ban Dân tộc ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động cơ quan Ban Dân tộc tỉnh Khánh Hoà.

Điều 3. Chánh Văn phòng; các Trưởng, phó phòng và cán bộ, công chức thuộc Ban Dân tộc chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Lãnh đạo Ban;
- Lưu: VT.

TRƯỞNG BAN

Ký bởi: Đặng Văn Tuấn
Email: dvtuan@khanhhoa.gov.vn
Cơ quan: Ban Dân tộc, Tỉnh Khánh Hòa
Ngày ký: 28.12.2018 13:58:30 +07:00

Đặng Văn Tuấn

UBND TỈNH KHÁNH HÒA
BAN DÂN TỘC

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

QUY CHẾ
Đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc

(Ban hành kèm theo Quyết định số 105/QĐ-BDT ngày 28/12/2018 của Trưởng Ban Dân tộc)

Chương I
QUY ĐỊNH CHUNG

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

1. Quy chế này quy định về đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc tỉnh Khánh Hoà.

2. Quy chế này áp dụng cho tất cả cán bộ, công chức thuộc Ban Dân tộc trong việc vận hành, khai thác và sử dụng hệ thống thông tin tại cơ quan.

Điều 2. Hệ thống thông tin của cơ quan

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.

2. Hệ thống thông tin của cơ quan phải tuân thủ các nguyên tắc đảm bảo an toàn thông tin số theo quy định tại Điều 41 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.

3. Trưởng ban là người có quyền cao nhất đối với toàn bộ hoạt động và công tác đảm bảo an toàn thông tin số cho hệ thống thông tin của cơ quan; có toàn quyền trong việc giao hay không giao quyền sử dụng, thu hồi quyền của người sử dụng trong hệ thống thông tin của cơ quan; có quyền quyết định việc sử dụng các thành phần của hệ thống thông tin ngoài mục đích phục vụ công việc trên cơ sở tuân thủ các quy định của pháp luật và chịu hoàn toàn trách nhiệm đối với quyết định của mình.

Điều 3. Nguyên tắc bảo đảm an toàn thông tin

1. Cán bộ, công chức chịu trách nhiệm trước pháp luật về nội dung thông tin đã chuyển đi trên mạng nội bộ (LAN), mạng truyền số liệu chuyên dùng của các cơ quan Đảng và Nhà nước (mạng WAN) và mạng Internet.

2. Tuân thủ các nguyên tắc, các tiêu chuẩn, quy chuẩn kỹ thuật về bảo mật, an toàn thông tin số; chấp hành hướng dẫn của cơ quan chuyên môn quản lý nhà nước về thông tin và truyền thông về các giải pháp, biện pháp, kỹ thuật về quản lý, bảo mật, an toàn thông tin số.

3. Các văn bản có nội dung "Mật" trở lên khi được soạn thảo phải trên thiết bị không kết nối mạng và được kiểm định; khi gửi, nhận qua mạng phải được thủ trưởng cơ quan, đơn vị cho phép và phải được mã hóa theo quy định của Luật cơ yếu và các văn bản pháp luật liên quan.

4. Kết hợp nhiều biện pháp bảo đảm an toàn thông tin số, nhằm phát hiện và ngăn chặn kịp thời các nguy cơ mất an toàn thông tin.

5. Công tác đảm bảo an toàn thông tin mạng phải được thực hiện trên cơ sở có sự phối hợp chặt chẽ giữa cơ quan, đơn vị và cá nhân.

Chương II
NỘI DUNG ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 4. Bảo vệ thông tin cá nhân

1. Cán bộ, công chức có trách nhiệm tự bảo vệ thông tin cá nhân của mình và tuân thủ các quy định tại khoản 1, khoản 2 Điều 10; khoản 1, khoản 4 Điều 16; khoản 3 Điều 17; khoản 1 Điều 18 Luật an toàn thông tin mạng và trong các văn bản pháp luật có liên quan.

Khi sử dụng, khai thác các hệ thống thông tin của cơ quan và các phần mềm ứng dụng dùng chung của tỉnh, có trách nhiệm:

a) Tự quản lý và chịu trách nhiệm về bảo vệ thông tin cá nhân đã được khai báo trong các hệ thống thông tin; không tiết lộ tài khoản đăng nhập, đấu nối, truy cập trái phép vào các phần mềm dùng chung của tỉnh.

b) Phải thực hiện việc đổi mật khẩu ngay sau khi được cấp tài khoản truy cập vào các phần mềm dùng chung của tỉnh. Mật khẩu phải thay đổi thường xuyên hoặc định kỳ 3 tháng 1 lần; không dùng một mật khẩu cho nhiều tài khoản.

c) Khi khai thác, sử dụng các phần mềm dùng chung của tỉnh tại các điểm truy cập Internet công cộng, tuyệt đối không đặt chế độ lưu trữ mật khẩu trong quá trình sử dụng.

2. Khi xử lý thông tin phải tuân thủ đầy đủ các nội dung theo quy định tại khoản 2, 3, 4, 5 Điều 16; khoản 1, 2 Điều 17; khoản 3 Điều 18; Điều 19 của Luật an toàn thông tin mạng và các quy định sau:

a) Quản lý và phân quyền truy cập trong các phần mềm ứng dụng, hệ thống thông tin, cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ, quyền hạn của người tham gia quản lý, vận hành, khai thác, sử dụng các phần mềm ứng dụng, hệ thống thông tin, cơ sở dữ liệu.

b) Cán bộ, công chức đã nghỉ việc hoặc chuyển công tác phải thực hiện việc thu hồi các thiết bị CNTT liên quan; đồng thời phải thông báo ngay bằng văn bản đến cơ quan quản lý, quản trị phần mềm ứng dụng, hệ thống thông tin, cơ sở dữ liệu để thực hiện các biện pháp kỹ thuật cập nhật lại, khóa hoặc hủy tài khoản người dùng.

Điều 5. Về quản lý, sử dụng hệ thống

1. Đối với thiết bị CNTT:

a) Công chức, người lao động có trách nhiệm quản lý trang thiết bị công nghệ thông tin (máy vi tính, máy in, thiết bị ngoại vi,...) được giao, tự quản lý dữ liệu trên máy tính của mình, tự quyết định việc chia sẻ tài nguyên với các máy tính khác theo đúng quy định.

Trong quá trình sử dụng các thiết bị CNTT, nếu có sự cố xảy ra, công chức, lao động lập phiếu yêu cầu sửa chữa, chuyển đến Văn phòng. Trong trường hợp xảy ra sự cố lớn phiếu yêu cầu sửa chữa phải được xác nhận của Trưởng ban.

b) Máy tính và các thiết bị CNTT để nơi an toàn, tránh ảnh hưởng các tác nhân bên ngoài (ánh nắng, mưa...), thường xuyên vệ sinh cho máy; hàng ngày kiểm tra theo dõi sự hoạt động của máy tính, thiết bị ngoại vi... Khi không sử dụng máy tính nên tắt máy nhằm tiết kiệm điện và phòng, chống các xâm nhập trái phép.

c) Máy tính chứa dữ liệu quan trọng và thường xuyên kết nối Internet phải cài đặt các phần mềm diệt virus tin cậy, có bản quyền.

d) Phụ trách công nghệ thông tin (Quản trị mạng) chịu trách nhiệm:

- Kiểm tra, theo dõi, đánh giá sự hoạt động của máy chủ, máy trạm, các thiết bị mạng và các thiết bị ngoại vi theo đúng tiêu chuẩn kỹ thuật; thực hiện việc sao lưu dữ liệu; ghi nhật ký báo lỗi của mạng, các thiết bị CNTT để thực hiện công tác bảo trì, bảo dưỡng định kỳ, đột xuất, giảm thiểu tối đa các sự cố kỹ thuật; cung cấp địa chỉ IP mạng và tham số mạng cho người dùng kết nối vào mạng diện rộng (WAN) của tỉnh.

- Quản lý kỹ thuật và duy trì hoạt động hệ thống thông tin của Ban; là đầu mối kết nối mạng LAN, mạng Internet, mạng dữ liệu chuyên dùng cho các phòng; kiểm tra hiện trạng, đề xuất sửa chữa hoặc mua mới các chủng loại thiết bị CNTT phù hợp, an toàn, bảo mật theo quy định về quản lý, sử dụng tài sản cơ quan. Hàng năm tham mưu đề xuất kế hoạch mua sắm thiết bị, máy móc, phần mềm an toàn, an ninh thông tin ở cơ quan.

2. Đối với hệ thống mạng WAN:

- Công chức, lao động khi tham gia vào mạng WAN 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 cho Quản trị mạng biết để xử lý.

- Quản trị mạng chịu tránh nhiệm cài đặt hệ thống an ninh mạng theo đúng tiêu chuẩn an toàn bảo mật; cài đặt hệ thống tự động cập nhật mẫu Virus mới và tự động diệt virus khi phát hiện có virus xâm nhập máy tính; thường xuyên kiểm tra, quét virus định kỳ cho tất cả các máy chủ, máy trạm; xử lý, khắc phục kịp thời khi xảy ra sự cố máy tính bị virus xâm nhập; đảm bảo hệ thống

mạng máy tính luôn sạch virus để đảm bảo máy tính của cán bộ, công chức, viên chức hoạt động tốt.

Điều 6. Quy định bảo vệ hệ thống thông tin mạng

1. Khi xây dựng, nâng cấp, mở rộng hạ tầng kỹ thuật CNTT, các hệ thống thông tin của cơ quan phải có phương án đảm bảo an toàn thông tin mạng và phải được Sở Thông tin và Truyền thông có ý kiến trước khi trình cấp có thẩm quyền phê duyệt.

2. Hệ thống mạng nội bộ (mạng LAN) được tổ chức theo hướng sử dụng máy chủ để quản lý các máy trạm trong hệ thống mạng, không sử dụng mô hình mạng ngang hàng (không có máy chủ quản lý), cài đặt hệ thống tường lửa (Firewall) để bảo vệ hệ thống mạng LAN. Các máy chủ, máy trạm, hệ thống lưu trữ nội bộ, thiết bị mạng, mạng không dây (wifi) phải được bảo vệ bởi mật khẩu an toàn. Tất cả các máy tính phải được cài đặt các phần mềm bảo vệ, phòng chống virus.

3. Khi thực hiện di chuyển các trang thiết bị CNTT lưu trữ dữ liệu, thông tin thuộc danh mục bí mật Nhà nước phải được tổ chức quản lý, giám sát chặt chẽ theo quy định của pháp luật về bảo vệ bí mật nhà nước.

4. Cập nhật kịp thời các bản vá lỗ hổng bảo mật từ nhà cung cấp, nhà sản xuất cho các hệ thống thông tin, cơ sở dữ liệu; có cơ chế sao lưu dữ liệu dự phòng, dữ liệu được lưu trữ tại nơi an toàn để sẵn sàng phục hồi cơ sở dữ liệu khi xảy ra sự cố an toàn thông tin mạng.

5. Khi thuê dịch vụ công nghệ thông tin ưu tiên việc đảm bảo an toàn thông tin.

6. Tổ chức phân quyền truy cập cho các đối tượng người dùng tham gia vận hành, khai thác các hệ thống thông tin đúng quy trình, chặt chẽ gắn với trách nhiệm của từng tổ chức, cá nhân để đảm bảo an toàn thông tin mạng cho các hệ thống thông tin cơ quan đang quản lý, vận hành.

7. Các cơ quan, đơn vị, cá nhân tham gia sử dụng mạng chuyên dùng thực hiện nghiêm túc các nội dung về đảm bảo an toàn thông tin mạng trên mạng truyền số liệu chuyên dùng được quy định tại các Điều 10, 11, 12 của Thông tư số 23/2011/TT-BTTTT ngày 11/8/2011 của Bộ Thông tin và Truyền thông.

8. Cập nhật và lưu trữ cấu hình chuẩn các thành phần của hệ thống, trước khi tiến hành cài đặt, thiết lập cấu hình lại hệ thống thông tin, đảm bảo duy trì hoạt động của hệ thống thông tin.

9. Cấu hình hệ thống thông tin cung cấp những chức năng cơ bản cho người dùng; thiết lập các chế độ phân quyền truy cập theo chỉ đạo của Trưởng ban.

10. Sử dụng mật khẩu: đặt cho tài khoản sử dụng ở dạng phức tạp (mật khẩu bao gồm chữ hoa, chữ thường trong bảng chữ cái, số và các ký tự đặc biệt), độ dài tối thiểu 8 ký tự. Không tiết lộ, chia sẻ mật khẩu cho người khác, khi kết

thúc công việc hoặc chuyển giao máy tính cho người khác sử dụng phải thoát khỏi tài khoản người dùng.

11. Phòng ngừa, phát hiện, ngăn chặn và xử lý phần mềm độc hại:

a) Tất cả các máy trạm, máy chủ, các thiết bị công nghệ thông tin trong mạng và hệ thống thông tin phải được cài đặt phần mềm phòng chống virus phù hợp. Các phần mềm phòng chống virus phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc, virus khi sao chép, mở các tập tin.

b) Cán bộ, công chức trong cơ quan phải được hướng dẫn về phòng chống phần mềm độc hại, các rủi ro do mã độc gây ra; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm trên máy trạm khi chưa có sự đồng ý của người có thẩm quyền theo quy định của cơ quan.

c) Tất cả các máy tính của cơ quan, đơn vị phải được cấu hình nhằm vô hiệu hóa tính năng tự động thực thi các tập tin trên các thiết bị lưu trữ di động.

d) Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại, virus trên máy chủ, máy trạm, thiết bị công nghệ thông tin như: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống virus, mất dữ liệu, những dấu hiệu bất thường khác,… người sử dụng phải giữ nguyên hiện trạng máy tính, không thực hiện bất cứ thao tác gì thêm nhằm tránh tình trạng thêm nghiêm trọng và báo trực tiếp cho cán bộ hoặc bộ phận có trách nhiệm của cơ quan, đơn vị để xử lý.

đ) Phòng ngừa hư hỏng, sự cố máy tính, hệ thống thông tin qua các sự cố bất khả kháng: hư hỏng thiết bị đột ngột, chập điện, cháy nổ, lũ lụt, sét đánh, trộm cắp, ...

12. Đảm bảo an toàn thông tin Trang thông tin điện tử:

- Nội dung cung cấp trên Trang thông tin điện tử của Ban Dân tộc bảo đảm đúng quy định tại Nghị định 43/2011/NĐ-CP ngày 13/6/2011 của Chính phủ quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử hoặc cổng thông tin điện tử của cơ quan nhà nước.

- Những vấn đề thông tin đối ngoại đăng tải thông tin theo quan điểm chỉ đạo của Đảng, Nhà nước; định hướng tuyên truyền của Bộ Ngoại giao, Ban Tuyên giáo Trung ương, Ban Tuyên giáo Tỉnh ủy. Khi khai thác, đăng tải liên quan đến vấn đề biên giới, biển, đảo phải trích dẫn nguồn tin chính thống, tuân thủ các quy định của pháp luật trong lĩnh vực hoạt động báo chí và bản quyền.

- Định kỳ thay đổi và quản lý bảo mật tài khoản của những người có quyền quản trị hệ thống.

Điều 7. Giải quyết và khắc phục sự cố về an toàn, an ninh thông tin

1. Đối với cán bộ, công chức:

a) Thông tin kịp thời cho Quản trị mạng và Văn phòng khi phát hiện các sự cố gây mất an toàn, an ninh thông tin trong hệ thống mạng.

b) Khi phát hiện hệ thống bị tấn công, thông qua các dấu hiệu khác thường như: hệ thống máy vi 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 ngoài (CD, USB, ổ cứng di động,...).

2. Đối với Quản trị mạng:

- Quản lý chặt chẽ việc di chuyển các trang thiết bị CNTT (máy chủ, máy trạm, thiết bị ngoại vi);

- 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 Chánh Văn phòng; đồng thời liên hệ với cơ quan chuyên môn (Sở Thông tin và Truyền thông) hướng dẫn khắc phục.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 8. Trách nhiệm của Lãnh đạo Ban

1. Phân công cán bộ, công chức chuyên trách hoặc phụ trách CNTT để quản lý kỹ thuật nghiệp vụ về an toàn thông tin tại cơ quan.

2. Tạo điều kiện để cán bộ, công chức chuyên trách hoặc phụ trách CNTT học tập, tiếp thu công nghệ, kiến thức an toàn thông tin.

3. Trang bị đầy đủ các kiến thức bảo mật cơ bản cho cán bộ, công chức trước khi cho phép truy nhập và sử dụng hệ thống thông tin.

4. Chỉ đạo các phòng chuyên chuyên môn thuộc Ban tăng cường công tác an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin.

5. Quan tâm đầu tư các thiết bị phần cứng, phần mềm liên quan đến công tác đảm bảo an toàn thông tin; phân bổ kinh phí duy trì hoạt động hệ thống thông tin hiệu quả; tạo điều kiện cho cán bộ, công chức tham gia lớp đào tạo nâng cao kiến thức công nghệ thông tin.

Điều 9. Trách nhiệm của cán bộ, công chức

1. Các máy tính khi không sử dụng trong thời gian dài (quá 2 giờ làm việc) 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.

2. Có trách nhiệm tự quản lý các thiết bị công nghệ thông tin được giao sử dụng; không tự ý thay đổi và tháo lắp các thiết bị trên máy vi tính khi chưa có sự đồng ý của Lãnh đạo Ban; không tự ý liên hệ với cá nhân bên ngoài vào can thiệp các thiết bị máy tính.

3. Trong trao đổi thông tin, dữ liệu phục vụ công việc, cán bộ, công chức phải sử dụng hệ thống thông tin do tỉnh Khánh Hoà (@khanhhoa.gov.vn), phần mềm quản lý văn bản eOffice. Hạn chế việc sử dụng các phương tiện trao đổi thông tin dữ liệu, hệ thống thư điện tử công cộng, mạng xã hội trên Internet trong hoạt động của Ban Dân tộc.

4. 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 gây mất mát thông tin.

5. Nghiêm chỉnh 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 toàn, an ninh thông tin tại cơ quan.

Điều 10. Những điều không được làm

1. Không được lợi dụng việc sử dụng Internet nhằm mục đích: Chống lại nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội; kích động bạo lực, đồi trụy, tệ nạn xã hội, mê tín dị đoan; phá hoại thuần phong mỹ tục của dân tộc.

2. Không được tiết lộ bí mật nhà nước và các bí mật khác đã được pháp luật quy định.

3. Không được chơi các trò chơi trực tuyến (game online) hoặc các trò chơi khác trên Internet trong giờ làm việc.

4. Không được truy cập hoặc tải các trang website có nội dung đồi trụy, phản động, các chương trình không rõ nguồn gốc, các thông tin quảng cáo hấp dẫn.

5. Khi sử dụng hệ thống thư điện tử (Email) không được kích chuột vào bất cứ thư điện tử, tệp đính kèm, đường link, thư rác, thư quảng cáo nào không rõ nguồn gốc và không xác định được người gửi.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 11. Xử lý vi phạm

Công chức, lao động vi phạm Quy chế này, thì tuỳ theo tính chất, mức độ vi phạm có thể bị xử lý hành chính, xử lý kỷ luật hoặc các hình thức xử lý khác theo quy định hiện hành; nếu vi phạm gây thiệt hại lớn đến tài nguyên mạng, hệ thống thông tin của Ban thì phải chịu trách nhiệm bồi thường vật chất về những thiệt hại gây ra theo quy định của pháp luật hiện hành.

Điều 12. Trách nhiệm thi hành

1. Chánh Văn phòng; các trưởng, phó phòng có trách nhiệm tổ chức, hướng dẫn, đôn đốc công chức, lao động nghiêm túc thực hiện quy chế này.

2. Trong quá trình tổ chức thực hiện, nếu có vấn đề phát sinh mới hoặc khó khăn, vướng mắc, công chức, lao động phản ảnh về Văn phòng để tổng hợp, báo cáo Lãnh đạo Ban xem xét sửa đổi, bổ sung cho phù hợp./.

TRƯỞNG BAN

Ký bởi: Đặng Văn Tuấn
Email: dvtuan@khanhhoa.gov.vn
Cơ quan: Ban Dân tộc, Tỉnh Khánh Hòa
Ngày ký: 28.12.2018 13:58:41 +07:00

Đặng Văn Tuấn