UBND TỈNH NINH THUẬN **BAN DÂN TỘC**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 02 /QĐ-BDT	*Ninh Thuận, ngày 18 tháng 02 năm 2020*

QUYẾT ĐỊNH

Về việc ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc tỉnh Ninh Thuận

TRƯỞNG BAN DÂN TỘC TỈNH NINH THUẬN

Căn cứ Luật giao dịch điện tử ngày 29/11/2005;

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;

Căn cứ Nghị định số 72/2013/NĐ-CP ngày 15/7/2013 của Chính phủ quy định về việc quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng;

Căn cứ Quyết định số 55/2018/QĐ-UBND, ngày 13/7/2018 của Ủy ban nhân dân tỉnh Ninh Thuận về việc quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Ban Dân tộc tỉnh Ninh Thuân;

Xét đề nghị của Chánh Thanh tra Ban Dân tộc,

QUYẾT ĐỊNH:

Điều 1. Ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc tỉnh Ninh Thuận, gồm 6 Chương và 17 Điều.

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

Điều 3. Chánh Thanh tra, Trưởng phòng chuyên môn thuộc Ban cùng toàn thể cán bộ, công chức chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận: - Như Điều 3; - Lãnh đạo Ban; - Lưu: VT, TTr.	**TRƯỞNG BAN** BAN DÂN TỘC **Pi Năng Thị Thuỷ**

UBND TỈNH NINH THUẬN
BAN DÂN TỘC

CỘNG HÒA 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 công nghệ thông tin của Ban Dân tộc tỉnh Ninh Thuận

(Ban hành kèm theo Quyết định số 02 /QĐ-BDT ngày 18/02/2020 của Ban Dân tộc tỉnh Ninh Thuận)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

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

Điều 2. Đối tượng áp dụng

Quy chế này áp dụng đối với tất cả các phòng; cán bộ, công chức tham gia vận hành, khai thác các hệ thống thông tin của Ban Dân tộc.

Điều 3. Giải thích từ ngữ

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

1. Mạng: Là khái niệm chỉ mạng viễn thông cố định, di động, Internet và mạng máy tính.

2. Tài khoản: Bao gồm tên tài khoản và mật khẩu của người sử dụng.

3. 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.

4. An toàn thông tin: Là sự bảo vệ thông tin và 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.

5. Phần mềm độc hại: Là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hoặc 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.

6. Người sử dụng: Cán bộ, công chức.

7. Cán bộ quản trị mạng: Là cán bộ được giao phụ trách công tác đảm bảo hạ tầng, ứng dụng, cơ sở dữ liệu và an toàn, an ninh thông tin cho việc triển khai, vận hành, khai thác hệ thống CNTT tại Ban Quản lý.

Chương II
NỘI DUNG BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 4. Các biện pháp quản lý kỹ thuật cơ bản trong công tác bảo đảm an toàn thông tin

1. Tổ chức mô hình mạng: Cài đặt, cấu hình, tổ chức hệ thống mạng theo mô hình mạng ngang hàng. Khi thiết lập các dịch vụ trên môi trường mạng Internet, chỉ cung cấp những chức năng thiết yếu nhất bảo đảm duy trì hoạt động của hệ thống thông tin; hạn chế sử dụng chức năng, cổng giao tiếp mạng, giao thức và các dịch vụ không cần thiết.

2. Quản lý hệ thống mạng không dây (Wireless LAN): Khi thiết lập mạng không dây, cần thiết lập các thông số an toàn và định kỳ ít nhất 3 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật.

3. Tổ chức quản lý tài khoản: Tiến hành rà soát ít nhất 6 tháng một lần các tài khoản và định danh người dùng trong hệ thống thông tin. Hủy tài khoản, quyền truy nhập hệ thống thông tin, thu hồi lại tất cả các tài sản liên quan tới hệ thống thông tin (khóa, thẻ nhận dạng, thư mục lưu trữ,…) đối với người sử dụng không còn công tác hoặc không còn sử dụng do được cấp tài khoản mới.

4. Quản lý đăng nhập hệ thống: Các hệ thống thông tin cần giới hạn số lần đăng nhập vào hệ thống, tự động khóa tài khoản khi liên tục đăng nhập sai vượt quá số lần quy định. Tổ chức theo dõi, giám sát tất cả các phương pháp đăng nhập từ xa, nhất là các trường hợp đăng nhập vào hệ thống với mục đích quản trị.

5. Chống phần mềm độc hại: Triển khai các phần mềm chống mã độc trên các máy tính, thiết bị di động trong mạng để phát hiện, loại trừ phần mềm độc hại. Thường xuyên cập nhật các phiên bản mới, các bản vá lỗi của các phần mềm chống virus để bảo đảm chương trình quét virus của cơ quan trên các máy tính luôn được cập nhật mới nhất; thiết lập chế độ quét thường xuyên ít nhất tuần 01 lần. Thường xuyên cập nhật bản vá các lỗ hổng bảo mật của hệ điều hành và các phần mềm ứng dụng trên máy tính để hạn chế tối đa rủi ro mất an toàn thông tin.

6. Bảo đảm an toàn cho Trang thông tin điện tử: Thực hiện theo hướng dẫn tại Công văn số 2132/BTTTT-VNCERT ngày 18/7/2011 của Bộ Thông tin và Truyền thông về việc hướng dẫn đảm bảo an toàn thông tin cho các Cổng/Trang thông tin điện tử.

7. Thiết lập cơ chế sao lưu và phục hồi cho máy trạm: Máy trạm cần được thực hiện các biện pháp sao lưu dữ liệu, thông tin quan trọng nhằm phục vụ cho công tác phục hồi dữ liệu một cách nhanh nhất.

8. Xử lý khẩn cấp: Khi phát hiện hệ thống thông tin bị tấn công cần thực hiện các bước cơ bản sau:

a) Bước 1: Ngắt kết nối máy tính ra khỏi mạng;

b) Bước 2: Sao chép toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ (phục vụ cho hoạt động phân tích, điều tra);

c) Bước 3: Khôi phục hệ thống bằng cách chuyển dữ liệu sao lưu mới nhất để hệ thống hoạt động trở lại;

d) Bước 4: Chủ trì, phối hợp với các cơ quan liên quan thành lập đoàn kiểm tra an toàn thông tin định kỳ hàng năm hoặc kiểm tra đột xuất khi phát hiện có các dấu hiệu vi phạm an toàn thông tin.

Điều 5. Các biện pháp quản lý vận hành trong công tác bảo đảm an toàn thông tin

1. Đối với cán bộ chuyên trách Công nghệ thông tin (CNTT)

a) Triển khai, thực hiện các nội dung của Điều 4 Quy chế này;

b) Nắm vững và thực hiện nghiêm túc các quy định về bảo vệ bí mật Nhà nước. Thường xuyên tự cập nhật các kiến thức về an toàn thông tin, nguy cơ tiềm ẩn có thể gây mất thông tin và các biện pháp phòng tránh khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ;

c) Phối hợp chặt chẽ với cơ quan Công an trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn, an ninh thông tin.

2. Đối với người sử dụng

a) Thường xuyên cập nhật những chính sách, quy trình, thủ tục an toàn thông tin của đơn vị cũng như thực hiện những hướng dẫn về an toàn thông tin của cán bộ chuyên trách công nghệ thông tin;

b) Hạn chế việc sử dụng chức năng chia sẻ tài nguyên, khi sử dụng chức năng này cần bật thuộc tính bảo mật bằng mật khẩu và thực hiện việc thu hồi chức năng này khi đã sử dụng xong;

c) Các tài khoản đăng nhập hệ điều hành cần phải đặt mật khẩu, khi không sử dụng thì phải khóa tài khoản.

Chương III
QUY ĐỊNH BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 6. 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, các phòng phải báo cáo cho người có thẩm quyền. 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 xoá bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

Điều 7. Quy định về cấp phát, thu hồi, cập nhật và quản lý các tài khoản truy cập vào hệ thống thông tin

Cán bộ quản trị mạng quản lý, cấp tài khoản cá nhân và phân quyền truy cập cho người sử dụng trên tất cả các máy trạm đặt tại các phòng thuộc Ban. 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.

Điều 8. Cơ chế sao lưu dữ liệu

1. Cán bộ quản trị mạng phối hợp với các đơn vị có liên quan thực hiện xác định các thông tin, thực hiện quy trình sao lưu dự phòng và phục hồi cho các phần mềm, dữ liệu cần thiết theo quy định, quy trình sao lưu, lưu trữ hiện có.

2. Dữ liệu sao lưu phải được lưu trữ an toàn trên Hệ thống lưu trữ dự phòng, thiết bị lưu trữ ngoài và được kiểm tra thường xuyên đảm bảo sẵn sàng cho việc sử dụng khi cần; việc kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu tối thiểu 6 tháng một lần (hoặc khi có yêu cầu đột xuất).

Điều 9. Cơ chế thông tin, báo cáo 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 quản trị mạng 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;

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

2. Đối với cán bộ quản trị mạng

a) Áp dụng mọi biện pháp để khắc phục và hạn chế thiệt hại do sự cố xảy ra, lập biên bản báo cáo lãnh đạo Ban;

b) Cung cấp đầy đủ, chính xác, kịp thời những thông tin cần thiết; thực hiện theo đúng hướng dẫn và tạo điều kiện thuận lợi cho cơ quan chức năng (Công an tỉnh, Sở Thông tin và Truyền thông...) tham gia khắc phục sự cố.

Chương VI
TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN VÀ CHẾ ĐỘ BÁO CÁO KIỂM TRA ĐỊNH KỲ VÀ ĐỘT XUẤT

Điều 10. Trách nhiệm của Trưởng ban

1. Trưởng ban chịu trách nhiệm trước UBND tỉnh trong công tác đảm bảo an toàn hệ thống thông tin của Ban Dân tộc;

2. Khi có sự cố hoặc nguy cơ mất an toàn thông tin, kịp thời sử dụng cán bộ chuyên trách về an toàn, an ninh thông tin của cơ quan áp dụng mọi biện pháp kỹ thuật để khắc phục, hạn chế thấp nhất mức thiệt hại có thể xảy ra;

3. Tạo điều kiện thuận lợi cho các cơ quan chức năng tham gia khắc phục sự cố và thực hiện đúng theo hướng dẫn;

4. Phân công cán bộ chuyên trách về an toàn hệ thống thông tin, đảm bảo an ninh thông tin, bảo mật trước khi tiến hành các hoạt động quản lý, vận hành hệ thống thông tin. Tạo điều kiện cho cán bộ chuyên trách được học tập, tiếp thu công nghệ và kiến thức về an toàn bảo mật thông tin;

5. Tổng hợp tình hình an toàn, an ninh thông tin và bảo mật của hệ thống thông tin theo định kỳ hàng năm để tổng hợp báo cáo Sở Thông tin và Truyền thông và UBND tỉnh.

Điều 11. Trách nhiệm của lãnh đạo các Phòng thuộc Ban

Phổ biến, tổ chức triển khai thực hiện tốt các quy định tại quy chế này đối với toàn thể cán bộ, công chức trong Phòng. Khi gặp sự cố cần phối hợp với Sở Thông tin và Truyền thông cung cấp thông tin và tạo điều kiện cho các đơn vị có chức năng triển khai công tác kiểm tra khắc phục kịp thời, nhanh chóng và đạt hiệu quả.

Điều 12. Trách nhiệm của Người sử dụng

1. Nghiêm chỉnh chấp hành các quy định, quy trình về an toàn, an ninh thông tin của cơ quan cũng như quy định khác của pháp luật, nâng cao ý thức cảnh giác và trách nhiệm bảo đảm an toàn, an ninh thông tin tại cơ quan, đơn vị.

2. Khi phát hiện sự cố phải báo ngay với lãnh đạo Phòng và cán bộ quản trị mạng để kịp thời ngăn chặn, xử lý.

3. Hưởng ứng, tham gia các chương trình đào tạo, hội nghị về an toàn, an ninh thông tin do Sở Thông tin và Truyền thông tổ chức (nếu có).

4. Có trách nhiệm quản lý, bảo quản thiết bị được giao sử dụng; không tự ý thay đổi cấu hình hoặc tháo lắp các thiết bị trên máy tính khi chưa có sự đồng ý của Lãnh đạo cơ quan, đơn vị.

Điều 13. Trách nhiệm của cán bộ quản trị mạng

1. Cán bộ quản trị mạng: Là cán bộ do Lãnh đạo Ban phân công, chịu trách nhiệm quản lý, vận hành các hoạt động hệ thống mạng máy tính. Tham mưu cho Lãnh đạo Ban trong việc đầu tư thiết bị phần cứng, phần mềm, công tác bảo mật thông tin trên môi trường mạng; sử dụng phần mềm có bản quyền và phần mềm mã nguồn mở cho hệ thống máy tính; cập nhật cấu hình chuẩn cho các thành phần của hệ thống khi tiến hành cài đặt và thiết lập cấu hình chặt chẽ nhất cho các sản phẩm an toàn thông tin nhưng vẫn duy trì yêu cầu hoạt động của hệ thống thông tin.

2. Sao chép, lưu trữ thông tin tại nơi an toàn; kiểm tra thông tin sao lưu để đảm bảo tính sẵn sàng và toàn vẹn của thông tin. Xử lý các sự cố về an toàn, an ninh thông tin và bảo mật hệ thống thông tin.

3. Triển khai các biện pháp chống virus, thư rác cho các máy trạm, các thiết bị di động trong mạng của cơ quan. Sử dụng biện pháp chống virus, thư rác để phát hiện và loại trừ những đoạn mã độc (virus, trojan.,.) được truyền tải bởi: thư điện tử, tập tin đính kèm từ Internet, thiết bị lưu trữ tháo lắp để khai thác lỗ hổng của hệ thống thông tin, Thường xuyên cập nhật các phần mềm chống virus, thư rác, bản vá lỗi hệ thống và hướng dẫn người dùng (user) sử dụng chương trình để bảo vệ an toàn dữ liệu.

4. Theo dõi và quản lý hoạt động hệ thống mạng, đề xuất lựa chọn công nghệ và triển khai các giải pháp nhằm đảm bảo cho hệ thống mạng cục bộ (LAN) hoạt động thông suốt, đảm bảo an toàn và bảo mật các thông tin truyền dẫn cho hệ thống mạng máy tính và đảm bảo hệ thống mạng LAN luôn được kết nối, hoạt động thông suốt.

5. Xây dựng quy trình, thử nghiệm, trực tiếp cài đặt, quản lý các phần mềm hệ thống và phần mềm ứng dụng trong hệ thống mạng máy tính; nghiên cứu, đề xuất, nâng cấp công nghệ phần mềm theo định hướng quản lý Nhà nước của ngành và tuân theo quy định của Chính phủ. Lắp đặt, hướng dẫn sử dụng, nâng cấp, cập nhật, bảo trì và quản trị mạng máy tính đảm bảo hoạt động ổn định và an toàn cho người sử dụng. Kiểm tra và xử lý các lỗi kỹ thuật đảm bảo việc truyền, nhận thông tin thông suốt giữa các Phòng thuộc Ban. Giữ bí mật tuyệt đối các thông tin trên mạng.

6. Thực hiện việc đánh giá, báo cáo và đề xuất với Lãnh đạo Ban các biện pháp phòng chống các rủi ro và mức độ nghiêm trọng của rủi ro đối với hệ thống thông tin của cơ quan (các rủi ro có thể xảy ra do sự truy cập, sử dụng thông tin trái phép; mất thông tin; thay đổi hoặc phá hủy thông tin của hệ thống).

Điều 14. Chế độ báo cáo, kiểm tra định kỳ và đột xuất

1. Định kỳ hàng năm, Ban Dân tộc báo cáo tình hình an toàn, an ninh thông tin gửi Sở Thông tin và Truyền thông theo quy định.

2. Phối hợp với Sở Thông tin và Truyền thông và các đơn vị có liên quan tiến hành kiểm tra công tác đảm bảo an toàn, an ninh thông tin mạng.

3. Phối hợp với đoàn kiểm tra tiến hành kiểm tra đột xuất các Phòng, chuyên môn có dấu hiệu vi phạm an toàn, an ninh thông tin.

Chương V
KHEN THƯỞNG, XỬ LÝ VI PHẠM

Điều 15. Khen thưởng

Các phòng thuộc Ban; cán bộ, công chức thực hiện tốt Quy chế này sẽ được xem xét đánh giá khen thưởng vào cuối năm.

Điều 16. Xử lý vi phạm

Các phòng thuộc Ban; cán bộ, công chức có hành vi vi phạm quy chế này thì tùy theo tính chất, mức độ vi phạm bị xử lý kỷ luật. Nếu gây thiệt hại có tính

chất nghiêm trọng thì phải bồi thường về vật chất và bị truy cứu trách nhiệm hình sự theo quy định của Pháp luật hiện hành.

Chương VI
TỔ CHỨC THỰC HIỆN

Điều 17. Điều khoản thi hành

Trong quá trình thực hiện Quy chế này nếu phát hiện những điều không phù hợp, vướng mắc cần sửa đổi, bổ sung, các Phòng chuyên môn kịp thời báo cáo về Phòng Thanh tra để tổng hợp trình Lãnh đạo Ban xem xét, điều chỉnh, bổ sung cho phù hợp./.

TRƯỞNG BAN

BAN DÂN TỘC

Pi Năng Thị Thuỷ