ỦY BAN DÂN TỘC	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Số: 466 /QĐ-UBDT	Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 02 tháng 10 năm 2013

QUYẾT ĐỊNH

Ban hành Quy chế đảm bảo an ninh, an toàn trên mạng thông tin trong hoạt động của Ủy ban Dân tộc

BỘ TRƯỞNG, CHỦ NHIỆM ỦY BAN DÂN TỘC

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

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về việc ứng dụng công nghệ thông tin trong hoạt động của cơ quan Nhà nước;

Căn cứ Nghị định số 84/2012/NĐ-CP ngày 12/10/2012 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Uỷ ban Dân tộc;

Căn cứ Thông tư liên tịch số 06/2008/TTLT/BTTTT-BCA ngày 28/11/2008 của liên Bộ Thông tin và Truyền thông và Bộ Công an về bảo đảm an toàn cơ sở hạ tầng và an ninh thông tin trong hoạt động bưu chính, viễn thông và công nghệ thông tin;

Căn cứ Thông tư số 23/2011/TT-BTTTT ngày 11/8/2011 của Bộ Thông tin và Truyền thông Quy định về việc quản lý, vận hành, sử dụng và bảo đảm an toàn thông tin trên Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;

Xét đề nghị của Giám đốc Trung tâm Thông tin,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an ninh, an toàn trên mạng thông tin trong hoạt động của Ủy ban Dân tộc

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

Điều 3. Giám đốc Trung tâm Thông tin, Chánh Văn phòng Uỷ ban, Thủ trưởng các Vụ, đơn vị và công chức, viên chức, người lao động thuộc Uỷ ban chịu trách nhiệm thi hành Quyết định này.

Nơi nhận:
- Như Điều 3;
- Bộ Thông tin và Truyền thông;
- Bộ trưởng, Chủ nhiệm UBDT;
- Các Thứ trưởng, PCN UBDT;
- Cổng TTĐT UBDT;
- Lưu: VT, TTTT.

KT.BỘ TRƯỞNG, CHỦ NHIỆM
THỨ TRƯỞNG, PHÓ CHỦ NHIỆM

Phan Văn Hùng

ỦY BAN DÂN TỘC

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

QUY CHẾ
Đảm bảo an ninh, an toàn trên mạng thông tintrong hoạt động của Ủy ban Dân tộc

(Ban hành kèm theo Quyết định số 466/QĐ-UBDT ngày 02 tháng 10 năm 2013 của Bộ trưởng, Chủ nhiệm Ủy ban Dân tộc)

Chương I
QUY ĐỊNH CHUNG

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

1. Quy chế này quy định việc sử dụng, quản lý khai thác, bảo vệ an ninh, an toàn trên mạng thông tin trong hoạt động của cơ quan Ủy ban Dân tộc.

2. Quy chế này áp dụng đối với các Vụ, đơn vị (sau đây gọi là đơn vị) thuộc Ủy ban Dân tộc và các cán bộ, công chức, viên chức, người lao động (sau đây gọi là CCVC) đang làm việc tại các đơn vị được quyền khai thác, sử dụng tài nguyên trên mạng thông tin của Ủy ban Dân tộc

Điều 2. Mục đích đảm bảo an ninh, an toàn trên mạng thông tin

1. Thực hiện bảo vệ bí mật nhà nước, giảm thiểu, phòng, chống các nguy cơ gây sự cố mất an toàn thông tin và đảm bảo an ninh thông tin trong quá trình tham gia hoạt động trên môi trường mạng.

2. Công tác đảm bảo an ninh thông tin, bảo mật trên môi trường mạng là một trong những nhiệm vụ trọng tâm để đảm bảo thành công trong việc ứng dụng công nghệ thông tin tại các đơn vị.

Điều 3. Giải thích từ ngữ

1. Mạng Ủy ban Dân tộc: Là tên viết tắt của hệ thống mạng thông tin của Ủy ban.

2. Người sử dụng: Là CCVC của các đơn vị trực thuộc Ủy ban Dân tộcđược quyền khai thác, sử dụng tài nguyên trên mạng thông tin của Uỷ ban Dân tộc.

3. An toàn thông tin: Bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin đối với nguy cơ tự nhiên hoặc do con người gây ra.

Bảo đảm cho các hệ thống thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy.

4. Tính tin cậy: Đảm bảo thông tin chỉ có thể được truy nhập bởi những người được cấp quyền sử dụng.

5. Tính toàn vẹn: Bảo vệ sự chính xác và đầy đủ của thông tin và các phương pháp xử lý.

6. Tính sẵn sàng: Đảm bảo những người được cấp quyền có thể truy nhập thông tin và các tài sản liên quan ngay khi có nhu cầu.

7. Hệ thống an ninh mạng: Là tập hợp các thiết bị tin học hoạt động đồng bộ theo một chính sách an ninh mạng nhất quán nhằm quản lý, giám sát, kiểm soát chặt chẽ các hoạt động trên mạng, phát hiện và xử lý các truy cập bất hợp pháp.

8. Hệ thống công nghệ thông tin: Là một tập hợp có cấu trúc các trang thiết bị phần cứng, phần mềm, cơ sở dữ liệu và hệ thống mạng phục vụ cho một hoặc nhiều hoạt động kỹ thuật, nghiệp vụ của Ủy ban Dân tộc.

9. Tài sản công nghệ thông tin: Là các trang thiết bị, thông tin thuộc hệ thống công nghệ thông tin của Ủy ban Dân tộc. Bao gồm:

a) Tài sản hữu hình: Là các thiết bị công nghệ thông tin, phương tiện truyền thông và các thiết bị phục vụ cho hoạt động của hệ thống công nghệ thông tin;

b) Tài sản thông tin: Là các dữ liệu, tài liệu liên quan đến hệ thống công nghệ thông tin. Tài sản thông tin được thể hiện bằng văn bản giấy hoặc dữ liệu điện tử;

c) Tài sản phần mềm: Bao gồm các chương trình ứng dụng, phần mềm hệ thống, cơ sở dữ liệu và công cụ phát triển.

10. Rủi ro công nghệ thông tin: Là khả năng xảy ra tổn thất khi thực hiện các hoạt động liên quan đến hệ thống công nghệ thông tin. Rủi ro công nghệ thông tin liên quan đến quản lý, sử dụng phần cứng, phần mềm, truyền thông, giao diện hệ thống, vận hành và con người.

11. Quản lý rủi ro: Là các hoạt động phối hợp nhằm xác định và kiểm soát các rủi ro công nghệ thông tin có thể xảy ra.

12. Bên thứ ba: Là các tổ chức, cá nhân có chuyên môn được đơn vị thuê hoặc hợp tác với đơn vị nhằm cung cấp hàng hóa, dịch vụ kỹ thuật cho hệ thống công nghệ thông tin.

13. Tường lửa: Là tập hợp các thành phần hoặc một hệ thống các trang thiết bị, phần mềm được đặt giữa hai mạng, nhằm kiểm soát tất cả các kết nối từ bên trong ra bên ngoài mạng hoặc ngược lại.

14. Vi rút: Là chương trình máy tính có khả năng lây lan, gây ra hoạt động không bình thường cho thiết bị số hoặc sao chép, sửa đổi, xóa bỏ thông tin lưu trữ trong thiết bị số.

15. Phần mềm độc hại (mã độc): Là các phần mềm có tính năng gây hại như vi rút, phần mềm do thám (spyware), phần mềm quảng cáo (adware) hoặc các dạng tương tự khác.

16. Điểm yếu kỹ thuật: Là vị trí trong hệ thống công nghệ thông tin dễ bị tổn thương khi bị tấn công hoặc xâm nhập bất hợp pháp.

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

Điều 4. Trang thiết bị và hạ tầng công nghệ thông tin

1. Hạ tầng mạng nội bộ

a) Hệ thống mạng có dây:

Hệ thống mạng nội bộ của các đơn vị phải được thiết kế thành một thể thống nhất, cùng kết hợp và hỗ trợ, tương tác hoạt động với nhau. Mô hình mạng tại hệ thống máy chủ phải được đảm bảo đầy đủ chia thành ba vùng gồm: Vùng ngoài, vùng máy chủ (DMZ), vùng làm việc. Hệ thống mạng tại mỗi đơn vị phải được xây dựng theo mô hình miền (Domain) nhằm mục đích quản lý hệ thống chặt chẽ, an toàn và bảo mật;

Các thiết bị mạng, máy chủ, được đặt riêng biệt trong phòng máy chủ để đảm bảo tính an toàn, bảo mật và tập trung, tạo thuận lợi cho việc quản trị hệ thống. Máy chủ phải được đặt trong vùng DMZ của bức tường lửa. Thiết bị chuyển mạch lớp 3 (switch layer 3) đóng vai trò trung tâm kết nối của hệ thống mạng, thiết bị chuyển mạch lớp 3 được đặt tại phòng máy chủ kết nối các thiết bị chuyển mạch lớp 2 đặt tại mỗi tầng của đơn vị tạo thành hệ thống mạng nội bộ tổng thể.

b) Hệ thống mạng không dây:

Ngoài giải pháp mạng có dây, có thể xây dựng giải pháp mạng nội bộ kết hợp với mạng không dây. Hệ thống mạng không dây phải đảm bảo kết nối tốt với các thiết bị đầu cuối và được bảo mật truy cập theo chuẩn bảo mật mạng không dây an toàn nhất. Quản lý chặt chẽ việc cấp phát tài khoản truy cập mạng không dây thông qua mật khẩu bảo vệ, mật khẩu phải được thay đổi định kỳ mỗi tháng ít nhất một lần. Thực hiện việc xác thực người sử dụng thông

qua: Họ tên người dùng, tên thiết bị dùng truy cập, mã số của thiết bị dùng truy cập.

2. Hệ thống máy chủ

a) Cấu hình máy chủ phải đủ mạnh để đáp ứng công việc. Máy chủ của Ủy ban và các đơn vị trực thuộc chỉ dùng để triển khai các phần mềm hệ thống, cài đặt các phần mềm dùng chung, các cơ sở dữ liệu cần thiết và các phần mềm chống virus, ngoài ra không được cài thêm bất cứ phần mềm nào khác. Hệ điều hành và các phần mềm ứng dụng hợp lệ cài đặt trên máy chủ phải có bản quyền của nhà cung cấp, không được sử dụng các phần mềm vi phạm bản quyền, phần mềm bẻ khóa.

b) Phòng máy chủ của Ủy ban Dân tộc phải độc lập và được Trung tâm Thông tin trực tiếp quản lý, người không được giao quản lý không được vào phòng máy chủ. Phòng máy chủ phải đảm bảo khô, thoáng, nguồn điện cung cấp ổn định, được trang bị máy lạnh và vận hành máy lạnh liên tục.

3. Thiết bị mạng, bảo mật, tường lửa

a) Thiết bị mạng phải được cung cấp từ các hãng sản xuất lớn có uy tín, đáp ứng nhiều kết nối truy cập cùng một thời điểm, phải hỗ trợ cơ chế cân bằng tải hạn chế việc tắc nghẽn đường truyền, hỗ trợ công nghệ ảo hóa. Các thiết bị phải đảm bảo khả năng cung cấp các chức năng quản trị nhằm tăng cường độ an toàn và bảo mật cho hệ thống mạng như: Hỗ trợ chức năng phân vùng truy cập, xác thực thiết bị và người sử dụng.

b) Thiết bị bảo mật phải có hệ thống tường lửa phát hiện và từ chối các truy cập không hợp lệ, có cơ chế ngăn chặn và sàng lọc các gói tin có nội dung xấu, hỗ trợ việc lưu lịch sử truy cập mạng và mã hóa mọi thông tin ra vào trong hệ thống mạng của Ủy ban Dân tộc. Hệ thống tường lửa phải có khả năng phát hiện và bảo vệ hệ thống trước các hình thức tấn công mạng phổ biến hiện nay như : Tấn công từ chối dịch vụ (DoS), tấn công bằng các gói tin không hợp lệ.

4. Xác định trách nhiệm đối với tài sản công nghệ thông tin

a) Thống kê, kiểm kê các loại tài sản công nghệ thông tin tại đơn vị mỗi năm tối thiểu một lần. Nội dung thống kê tài sản phải bao gồm các thông tin: Loại tài sản, giá trị, mức độ quan trọng, vị trí lắp đặt, thông tin dự phòng, thông tin về bản quyền.

b) Phân loại, sắp xếp thứ tự ưu tiên theo giá trị, mức độ quan trọng của tài sản công nghệ thông tin để có biện pháp bảo vệ tài sản phù hợp. Xây dựng và thực hiện các quy định về quản lý, sử dụng tài sản.

c) Gắn quyền sử dụng tài sản cho các cá nhân hoặc bộ phận cụ thể. Người sử dụng tài sản công nghệ thông tin phải tuân thủ các quy định về quản lý, sử dụng tài sản, đảm bảo tài sản được sử dụng đúng mục đích.

5. Phân loại tài sản công nghệ thông tin

a) Phân loại tài sản thông tin theo các tiêu chí về giá trị, độ nhạy cảm và tầm quan trọng, tần suất sử dụng, thời gian lưu trữ.

b) Thực hiện các biện pháp quản lý phù hợp với từng loại tài sản thông tin đã phân loại.

Điều 5. Đảm bảo an toàn thông tin trong đầu tư dự án công nghệ thông tin và xây dựng phần mềm

1. Yêu cầu về an toàn, bảo mật cho các hệ thống thông tin

Khi xây dựng hệ thống thông tin mới hoặc cải tiến hệ thống thông tin hiện tại, phải đưa ra các yêu cầu về an toàn, bảo mật cả về mặt ứng dụng và các tài liệu sử dụng trong quá trình xây dựng.

2. Yêu cầu về đảm bảo an toàn, bảo mật các ứng dụng

Các chương trình phần mềm ứng dụng phải đáp ứng các yêu cầu sau:

- Kiểm soát được tính hợp lệ của dữ liệu nhập vào ứng dụng;

- Lưu trữ lịch sử sử dụng nhằm phát hiện thông tin sai lệch do các lỗi trong quá trình xử lý hoặc các hành vi sửa đổi thông tin có chủ ý;

- Có các biện pháp đảm bảo tính xác thực và bảo vệ sự toàn vẹn của dữ liệu được xử lý trong các ứng dụng;

- Kiểm tra tính hợp lệ của dữ liệu xuất ra từ các ứng dụng, đảm bảo quá trình xử lý thông tin của các ứng dụng là chính xác và hợp lệ.

3. Yêu cầu về quản lý mã hóa

a) Quy định và đưa vào sử dụng các biện pháp mã hóa và quản lý khóa theo các chuẩn quốc gia hoặc quốc tế đã được công nhận để bảo vệ thông tin của đơn vị.

b) Dữ liệu về mật khẩu quản trị hệ thống, mật khẩu người sử dụng và các dữ liệu nhạy cảm khác phải được mã hóa khi truyền lên mạng và khi lưu trữ.

c) Mật khẩu hệ thống, mật khẩu người sử dụng và các thông tin liên quan đến xác thực thông tin phải được thay đổi hàng tuần.

4. Yêu cầu về an toàn, bảo mật các tệp tin hệ thống

a) Phải có quy trình về quản lý, cài đặt, cập nhật các phần mềm, đảm bảo an toàn cho các tệp tin hệ thống.

b) Dữ liệu kiểm tra, thử nghiệm phải được lựa chọn, bảo vệ, quản lý và kiểm soát một cách thận trọng.

c) Mã nguồn của các chương trình phải được quản lý và kiểm soát chặt chẽ.

5. Yêu cầu về an toàn, bảo mật trong quy trình hỗ trợ và phát triển

a) Phải có quy định về quản lý và kiểm soát sự thay đổi hệ thống thông tin.

b) Khi thay đổi hệ điều hành phải kiểm tra và xem xét các ứng dụng nghiệp vụ quan trọng để đảm bảo hệ thống hoạt động ổn định, an toàn trên môi trường mới.

c) Việc sửa đổi các gói phần mềm phải được quản lý và kiểm soát chặt chẽ từ khâu lên kế hoạch đến triển khai, nghiệm thu.

d) Giám sát, quản lý chặt chẽ việc thuê mua phần mềm bên ngoài.

6. Yêu cầu về quản lý các điểm yếu về mặt kỹ thuật

a) Có quy định về việc đánh giá, quản lý và kiểm soát các điểm yếu kỹ thuật của các hệ thống công nghệ thông tin đang sử dụng. Định kỳ đánh giá, lập báo cáo về các điểm yếu kỹ thuật của các hệ thống công nghệ thông tin đang sử dụng.

b) Xây dựng và triển khai các giải pháp khắc phục các điểm yếu kỹ thuật, hạn chế các rủi ro liên quan.

Điều 6. Bảo vệ bí mật nhà nước trong 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 và nội bộ) để soạn thảo văn bản, chuyển giao, lưu trữ thông tin có nội dung bí mật nhà nước; không được cung cấp tin, bài, tài liệu và đưa thông tin bí mật nhà nước lên Trang tin điện tử/Cổng Thông tin điện tử (gọi tắt là Cổng Thông tin). Nghiêm cấm cài cắm các thiết bị lưu trữ tài liệu có nội dung bí mật nhà nước vào máy tính nối mạng Internet.

b) Không được in, sao chụp tài liệu, vật mang 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 để soạn thảo văn bản mật, các cơ quan phải chuyển cho Trung tâm Thông tin xử lý. Không được cho phép bất kỳ các công ty tư nhân hoặc người không có trách nhiệm

trực tiếp sửa chữa, xử lý và khắc phục các sự cố của máy tính dùng để soạn thảo văn bản mật.

3. Trước khi thanh lý các máy tính trong cơ quan, cán bộ chuyên trách công nghệ thông tin phải dùng các chương trình phần mềm xóa bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính. Không được thanh lý ổ cứng máy tính dùng soạn thảo và chứa các nội dung mật.

Điều 7. Đảm bảo an toàn cho Cổng Thông tin

1. Tài liệu thiết kế và mã nguồn phần mềm

Quản lý toàn bộ các phiên bản của mã nguồn và các tài liệu liên quan. Phối hợp với đơn vị cung cấp dịch vụ lưu trữ Cổng Thông tin đảm bảo an ninh bảo mật cho máy chủ lưu trữ Cổng Thông tin, tránh khả năng tấn công leo thang đặc quyền. Yêu cầu đơn vị cung cấp dịch vụ lưu trữ phải cài đặt các hệ thống phòng vệ như tường lửa, thiết bị phát hiện/phòng chống xâm phạm trái phép.

2. Vận hành ứng dụng Cổng Thông tin an toàn

a) Các Cổng Thông tin khi đưa vào sử dụng hoặc khi bổ sung thêm các chức năng, dịch vụ công mới cần đánh giá kiểm định nhằm tránh được các lỗi bảo mật thường xảy ra trên ứng dụng Cổng Thông tin.

b) Đơn vị phụ trách Cổng Thông tin phải đưa ra quy chế quản trị và cập nhật tin bài đảm bảo an toàn bảo mật trong quá trình quản trị và biên tập tin bài.

c) Máy tính và các thiết bị sử dụng cập nhật tin bài lên Cổng Thông tin phải được đảm bảo an toàn và phải cài đặt các phần mềm phòng chống virus, mã độc

3. Các biện pháp dự phòng thảm họa, sự cố

Phối hợp với các nhà cung cấp dịch vụ hosting xây dựng phương án phục hồi Cổng Thông tin, trong đó chú ý mỗi tháng thực hiện việc lưu trữ toàn bộ nội dung Cổng Thông tin một lần bao gồm mã nguồn, cơ sở dữ liệu, dữ liệu phi cấu trúc,... để bảo đảm khi có sự cố có thể khắc phục lại ngay trong vòng 24 giờ.

Điều 8. Đảm bảo an toàn thông tin trong quản lý, vận hành hệ thống công nghệ thông tin

1. Quy trình vận hành

a) Yêu cầu hệ thống vận hành chính thức:

- Tách biệt với môi trường phát triển và môi trường kiểm tra, thử nghiệm;

- Chỉ cho phép kết nối Internet đối với hệ thống công nghệ thông tin đã được áp dụng đầy đủ các giải pháp an ninh, an toàn và đủ khả năng bảo vệ trước các hiểm họa, tấn công từ bên ngoài;

- Không cài đặt các công cụ, phương tiện phát triển ứng dụng trên hệ thống vận hành chính thức;

- Hệ thống vận hành chính thức chỉ bao gồm các ứng dụng đã được đóng gói.

b) Ban hành và triển khai quy trình vận hành các hệ thống công nghệ thông tin đến người sử dụng bao gồm: Quy trình bật, tắt thiết bị; quy trình sao lưu, phục hồi dữ liệu; quy trình bảo dưỡng thiết bị; quy trình vận hành ứng dụng; quy trình xử lý sự cố.

c) Kiểm soát sự thay đổi của hệ thống công nghệ thông tin bao gồm: Các phiên bản phần mềm, cấu hình phần cứng, tài liệu, quy trình vận hành; phải có phương án dự phòng trong quá trình nâng cấp thay đổi hệ thống; ghi chép chi tiết các bước, nội dung thay đổi; lập kế hoạch thực hiện và kiểm tra, vận hành thử nghiệm hệ thống trước khi áp dụng chính thức.

d) Đối với hệ thống thông tin điều hành tác nghiệp:

- Mỗi nghiệp vụ phải được chia thành các luồng công việc khác nhau và phân quyền xử lý tới các cá nhân khác nhau;

- Không để một cá nhân làm toàn bộ các khâu từ khởi tạo đến phê duyệt một giao dịch nghiệp vụ;

- Mọi tác vụ trên hệ thống được lưu vết, sẵn sàng cho kiểm tra, kiểm soát khi cần thiết.

2. Quản lý các dịch vụ do bên thứ ba cung cấp

a) Phải giám sát và kiểm tra các dịch vụ do bên thứ ba cung cấp đảm bảo chất lượng dịch vụ, khả năng hoạt động hệ thống đáp ứng đúng quy trình nghiệp vụ, đáp ứng các yêu cầu về bảo mật .

b) Quản lý các thay đổi đối với các dịch vụ của bên thứ ba cung cấp bao gồm: Nâng cấp phiên bản mới; sử dụng các kỹ thuật mới, các công cụ và môi trường phát triển mới. Đánh giá đầy đủ tác động của việc thay đổi, đảm bảo an toàn khi được đưa vào sử dụng.

3. Quản lý việc lập kế hoạch và tiếp nhận hệ thống công nghệ thông tin

Giám sát việc lập kế hoạch công nghệ thông tin và xây dựng các yêu cầu, tiêu chuẩn về kỹ thuật, an toàn thông tin. Thực hiện kiểm tra đánh giá khả năng đáp ứng của hệ thống công nghệ thông tin mới hoặc hệ thống nâng cấp trước khi áp dụng chính thức.

4. Sao lưu dự phòng

a) Ban hành và phổ biến quy trình sao lưu dự phòng và phục hồi cho các phần mềm, dữ liệu cần thiết.

b) Lập danh sách các dữ liệu, phần mềm cần được sao lưu, có phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu.

c) Dữ liệu sao lưu phải được lưu trữ an toàn và được kiểm tra thường xuyên đảm bảo sẵn sàng cho việc sử dụng khi cần. Kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu tối thiểu ba tháng một lần.

5. Quản lý về an toàn, bảo mật mạng

a) Thực hiện việc quản lý và kiểm soát mạng nhằm ngăn ngừa các hiểm họa và duy trì an toàn cho các hệ thống, ứng dụng sử dụng mạng:

- Có sơ đồ logic và vật lý về hệ thống mạng;

- Sử dụng thiết bị tường lửa, thiết bị phát hiện và ngăn chặn xâm nhập và các trang thiết bị khác đảm bảo an toàn bảo mật mạng.

b) Thiết lập, cấu hình đầy đủ các tính năng của thiết bị an ninh mạng. Sử dụng các công cụ để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng và các truy cập bất hợp pháp vào hệ thống mạng. Thường xuyên kiểm tra, phát hiện những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào mạng.

c) Xác định và ghi rõ các tính năng an toàn, các mức độ bảo mật của dịch vụ và yêu cầu quản lý trong các thỏa thuận về dịch vụ mạng do bên thứ ba cung cấp.

6. Trao đổi thông tin

a) Ban hành các quy định trao đổi thông tin và phần mềm qua mạng truyền thông giữa các đơn vị trong Ủy ban và với các đơn vị bên ngoài. Xác định trách nhiệm và nghĩa vụ pháp lý với các thành phần tham gia.

b) Có thỏa thuận về an toàn bảo mật cho việc trao đổi thông tin với bên ngoài.

c) Có biện pháp bảo vệ phương tiện mang tin khi vận chuyển.

d) Xây dựng và thực hiện các biện pháp bảo vệ thông tin trao đổi giữa các hệ thống công nghệ thông tin.

7. Phòng chống vi rút và phần mềm độc hại

Xây dựng và thực hiện quy định về phòng chống vi rút, mã độc đáp ứng các yêu cầu cơ bản sau:

- Triển khai và thường xuyên nâng cấp hệ thống phòng chống vi rút máy tính cho toàn bộ hệ thống công nghệ thông tin của đơn vị;

- Kiểm tra, diệt vi rút, mã độc cho toàn bộ hệ thống công nghệ thông tin của đơn vị hàng ngày và phương tiện mang tin nhận từ bên ngoài trước khi sử dụng;

- Không mở các thư điện tử lạ, các tệp tin đính kèm hoặc các liên kết trong các thư lạ để tránh vi rút, mã độc;

- Không vào các Trang tin không có nguồn gốc xuất xứ rõ ràng, đáng ngờ;

- Cập nhật kịp thời các mẫu vi rút, mã độc mới và các phần mềm chống vi rút có bản quyền;

- Báo ngay cho người quản trị hệ thống xử lý trong trường hợp phát hiện nhưng không diệt được vi rút, mã độc;

- Không tự ý cài đặt các phần mềm khi chưa được kiểm định về tính an toàn bảo mật.

8. Giám sát và ghi nhật ký hoạt động của hệ thống công nghệ thông tin

a) Ghi nhật ký và quy định thời gian lưu trữ các thông tin về hoạt động của hệ thống công nghệ thông tin và người sử dụng, lỗi phát sinh và các sự cố mất an toàn thông tin nhằm trợ giúp cho việc điều tra giám sát về sau.

b) Xem xét và lập báo cáo định kỳ về nhật ký và có các hoạt động xử lý các lỗi, sự cố cần thiết.

c) Bảo vệ các chức năng ghi nhật ký và thông tin nhật ký, chống giả mạo và truy cập trái phép. Người quản trị hệ thống và người sử dụng không được xóa hay sửa đổi nhật ký hệ thống ghi lại các hoạt động của chính họ.

d) Có cơ chế đồng bộ thời gian giữa các hệ thống công nghệ thông tin.

Điều 9. Giải quyết và khắc phục sự cố công nghệ thông tin

1. Báo cáo sự cố

a) Đơn vị chuyên trách về công nghệ thông tin xây dựng quy trình báo cáo, các mẫu báo cáo và xác định rõ người nhận báo cáo về các sự cố công nghệ thông tin.

b) Quy định rõ trách nhiệm báo cáo của cán bộ, nhân viên và bên thứ ba về các sự cố công nghệ thông tin.

c) Các sự cố mất an toàn phải được lập tức báo cáo đến những người có thẩm quyền và những người có liên quan để có biện pháp khắc phục trong thời gian sớm nhất.

2. Kiểm soát và khắc phục sự cố

a) Ban hành quy trình, trách nhiệm khắc phục và phòng ngừa sự cố công nghệ thông tin, đảm bảo sự cố được xử lý trong thời gian ngắn nhất và giảm thiểu khả năng sự cố lặp lại.

b) Quá trình xử lý sự cố phải được ghi chép và lưu trữ tại đơn vị.

c) Thu thập, ghi chép, bảo toàn bằng chứng, chứng cứ phục vụ cho việc kiểm tra, xử lý, khắc phục và phòng ngừa sự cố. Trong trường hợp sự cố về công nghệ thông tin có liên quan đến các vi phạm pháp luật, đơn vị có trách nhiệm thu thập và cung cấp chứng cứ cho cơ quan có thẩm quyền đúng theo quy định của pháp luật.

3. Đảm bảo hoạt động liên tục

a) Căn cứ quy mô và mức độ quan trọng của từng hệ thống công nghệ thông tin đối với hoạt động của Ủy ban Dân tộc để lựa chọn ra các hệ thống công nghệ thông tin trọng yếu, có ảnh hưởng lớn tới hoạt động của đơn vị.

b) Xây dựng và triển khai kế hoạch, quy trình đảm bảo hoạt động liên tục của các hệ thống công nghệ thông tin trọng yếu.

c) Tối thiểu sáu tháng một lần, tiến hành kiểm tra, thử nghiệm, đánh giá và cập nhật các quy trình đảm bảo hoạt động liên tục của các hệ thống công nghệ thông tin trọng yếu.

d) Kế hoạch, quy trình đảm bảo hoạt động liên tục phải được kiểm tra, đánh giá và cập nhật khi có sự thay đổi của hệ thống.

4. Công tác dự phòng thảm họa

a) Xây dựng hệ thống dự phòng cho các hệ thống công nghệ thông tin trọng yếu của Ủy ban và các đơn vị trực thuộc.

b) Hệ thống dự phòng phải thay thế được hệ thống chính trong vòng 4 giờ kể từ khi hệ thống chính có sự cố không khắc phục được.

c) Tối thiểu ba tháng một lần, phải chuyển hoạt động từ hệ thống chính sang hệ thống dự phòng để đảm bảo tính đồng nhất và sẵn sàng của hệ thống dự phòng.

d) Tối thiểu ba tháng một lần, tiến hành kiểm tra, đánh giá hoạt động của hệ thống dự phòng.

Điều 10. Quản lý nguồn nhân lực nội bộ của đơn vị

1. Trước khi tuyển dụng hoặc phân công nhiệm vụ

a) Xác định trách nhiệm về an toàn, bảo mật công nghệ thông tin của vị trí cần tuyển dụng hoặc phân công.

b) Kiểm tra lý lịch, xem xét đánh giá nghiêm ngặt tư cách đạo đức, trình độ chuyên môn khi tuyển dụng, phân công cán bộ làm việc tại các vị trí trọng yếu của hệ thống công nghệ thông tin như quản trị hệ thống, quản trị hệ thống an ninh bảo mật, vận hành hệ thống, quản trị cơ sở dữ liệu.

c) Quyết định hoặc hợp đồng tuyển dụng (nếu có) phải bao gồm các điều khoản về trách nhiệm đảm bảo an toàn, bảo mật công nghệ thông tin của người được tuyển dụng trong và sau khi làm việc tại các đơn vị thuộc Ủy ban Dân tộc.

2. Trong thời gian làm việc

a) Lãnh đạo các đơn vị có trách nhiệm phổ biến và cập nhật các quy định về an toàn, bảo mật công nghệ thông tin cho CCVC của đơn vị mình.

b) Trung tâm Thông tin phải phối hợp với các đơn vị tiến hành kiểm tra việc thi hành các quy định về an toàn, bảo mật công nghệ thông tin của cá nhân, tổ chức thuộc đơn vị tối thiểu mỗi năm một lần.

c) Áp dụng các hình thức khen thưởng và kỷ luật đối với CCVC của đơn vị vi phạm quy định an toàn, bảo mật công nghệ thông tin.

d) Những công việc quan trọng như cấu hình hệ thống an ninh mạng, thay đổi tham số hệ điều hành, cài đặt thiết bị tường lửa, thiết bị phát hiện và ngăn chặn xâm nhập phải được thực hiện bởi ít nhất hai người hoặc phải có người giám sát.

đ) Không được cấp quyền quản trị (người có thể chỉnh sửa cấu hình, dữ liệu, nhật ký) trên hệ thống công nghệ thông tin chính và hệ thống dự phòng cho cùng một cá nhân.

3. Khi chấm dứt hoặc thay đổi công việc

Khi CCVC chấm dứt hoặc thay đổi công việc, đơn vị phải:

- Xác định rõ trách nhiệm của CCVC và các bên liên quan về hệ thống công nghệ thông tin;

- Làm biên bản bàn giao tài sản với CCVC;

- Thu hồi hoặc thay đổi quyền truy cập hệ thống công nghệ thông tin của CCVC cho phù hợp với công việc được thay đổi.

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

Điều 11. Trách nhiệm của Trung tâm Thông tin

1. Chủ trì tham mưu Lãnh đạo Ủy ban về công tác đảm bảo an ninh, an toàn thông tin và chịu trách nhiệm trước Lãnh đạo Ủy ban trong việc đảm bảo an ninh, an toàn thông tin cho các hệ thống thông tin tại Ủy ban Dân tộc (gồm các nội dung của Chương II).

2. Chủ trì và phối hợp với các cơ quan có liên quan thành lập đoàn kiểm tra công tác đảm bảo an ninh, an toàn thông tin; báo cáo Lãnh đạo Ủy ban về các hành vi vi phạm hành chính trong lĩnh vực công nghệ thông tin tại Ủy ban Dân tộc để xử lý theo quy định của pháp luật.

3. Xây dựng và triển khai các chương trình đào tạo, hội nghị tuyên truyền an ninh, an toàn thông tin trong công tác quản lý nhà nước.

4. Tùy theo mức độ sự cố, phối hợp với Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố thông tin.

5. Hướng dẫn các cơ quan, đơn vị xây dựng quy định đảm bảo an ninh, an toàn thông tin; hướng dẫn nội dung báo cáo định kỳ để các cơ quan, đơn vị thực hiện thống nhất.

6. Trung tâm Thông tin chủ trì triển khai cơ chế điều phối và phối hợp giữa các đơn vị nhằm đảm bảo an toàn an ninh thông tin trên Internet.

7. Phối hợp với các cơ quan báo chí đẩy mạnh tuyên truyền nâng cao nhận thức về an toàn an ninh thông tin trên mạng internet.

Điều 12. Trách nhiệm của cán bộ chuyên trách về công nghệ thông tin trong Ủy ban Dân tộc

1. Cán bộ chuyên trách về công nghệ thông tin chịu trách nhiệm tham mưu và vận hành an toàn hệ thống thông tin của đơn vị, tổ chức theo dõi, kiểm soát tất cả các phương pháp truy nhập từ xa tới hệ thống thông tin bao gồm cả sự truy nhập có chức năng đặc quyền. Hệ thống phải có quá trình kiểm tra, cho phép truy nhập từ xa và chỉ những người được phân quyền mới có quyền truy cập từ xa vào hệ thống. Đồng thời tổ chức triển khai cơ chế tự động giám sát và điều khiển các truy nhập từ xa.

2. Thường xuyên kiểm ra giám sát việc sao lưu dự phòng đảm bảo tính sẵn sàng và toàn vẹn của thông tin.

3. Tổ chức triển khai các biện pháp phòng, chống, lây nhiễm virus, mã độc, thư rác,... trong hệ thống thông tin.

4. Xây dựng cơ sở dữ liệu, thiết lập hệ thống an toàn thông tin có khả năng ngăn chặn các truy nhập bất hợp pháp và chỉ cho phép gửi/nhận các dữ liệu theo các địa chỉ hợp lệ.

5. Thường xuyên triển khai các biện pháp phòng chống rủi ro có thể xảy ra do truy cập, sử dụng trái phép; làm mất, thay đổi hoặc phá hủy hệ thống thông tin có liên quan tới hoạt động của đơn vị. Trường hợp xảy ra rủi ro cần

kịp thời tổng hợp, đánh giá và báo cáo mức độ nghiêm trọng để có các biện pháp xử lý kịp thời.

Điều 13. Trách nhiệm của các đơn vị thuộc Ủy ban Dân tộc

1. Lãnh đạo các đơn vị chịu trách nhiệm trước Lãnh đạo Ủy ban trong công tác đảm bảo an toàn hệ thống thông tin của đơn vị mình và có trách nhiệm thi hành và phổ biến quy chế này tới CCVC thuộc đơn vị mình.

2. Khi có sự cố hoặc nguy cơ mất an toàn thông tin, kịp thời áp dụng mọi biện pháp để khắc phục và hạn chế thấp nhất mức thiệt hại có thể xảy ra, báo cáo bằng văn bản cho cơ quan cấp trên quản lý trực tiếp và Trung tâm Thông tin của Ủy ban Dân tộc. Trường hợp có sự cố nghiêm trọng vượt quá khả năng khắc phục của đơn vị, phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và Trung tâm Thông tin để kịp thời khắc phục.

3. Phối hợp với Trung tâm Thông tin lên phương án dự phòng nhằm khắc phục sự cố và đảm bảo hệ thống hoạt động liên tục; 100% các ứng dụng giao dịch điện tử phải được đảm bảo về an toàn thông tin.

5. Lên kế hoạch đầu tư cần thiết để đảm bảo và tăng cường an ninh, an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của đơn vị.

6. Báo cáo định kỳ hàng quý tình hình an ninh, an toàn thông tin tại đơn vị mình, gửi về Trung tâm Thông tin để tổng hợp, báo cáo Lãnh đạo Ủy ban.

Điều 14. Trách nhiệm của CCVC trong Ủy ban

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

2. Khi phát hiện các nguy cơ mất an toàn hoặc sự cố phải báo cáo ngay cho bộ phận chuyên trách của cơ quan, đơn vị để kịp thời ngăn chặn, xử lý.

3. Tham gia các chương trình đào tạo, hội nghị về an ninh, an toàn thông tin do cơ quan cấp trên và Trung tâm Thông tin tổ chức.

Điều 15. Trách nhiệm trong công tác kiểm tra đảm bảo an ninh, an toàn thông tin

1. Trung tâm Thông tin chủ trì, phối hợp với các đơn vị có liên quan tiến hành kiểm tra công tác đảm bảo an ninh, an toàn thông tin định kỳ hàng năm đối với các đơn vị trong Ủy ban Dân tộc.

2. Các cơ quan liên quan được mời tham gia đoàn kiểm tra: Cử cán bộ có chuyên môn về công nghệ thông tin tham gia đoàn kiểm tra do Trung tâm Thông tin tổ chức; phối hợp với đoàn kiểm tra xây dựng các tiêu chí và quy trình kỹ thuật kiểm tra công tác đảm bảo an ninh, an toàn thông tin.

Chương IV
ĐIỀU KHOẢN THI HÀNH

Điều 16. Xử lý vi phạm

Tổ chức, cá nhân có hành vi vi phạm Quy chế này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật, xử phạt hành chính hoặc bị truy cứu trách nhiệm hình sự. Nếu gây thiệt hại thì phải bồi thường theo quy định hiện hành của pháp luật.

Điều 17. Trách nhiệm thi hành

1. Trung tâm Thông tin chủ trì, phối hợp với các đơn vị liên quan triển khai thực hiện Quy chế này.

2. Văn phòng Ủy ban có trách nhiệm phối hợp với Trung tâm Thông tin kiểm tra việc chấp hành Quy chế này.

3. Thủ trưởng các đơn vị thuộc Ủy ban Dân tộc trong phạm vi chức năng, nhiệm vụ của mình, có trách nhiệm tổ chức triển khai và kiểm tra việc chấp hành tại đơn vị theo đúng các quy định của Quy chế này.

Điều 18. Tổ chức thực hiện

Trong quá trình tổ chức thực hiện, nếu phát sinh những vấn đề khó khăn, vướng mắc cần sửa đổi, đề nghị các đơn vị thông báo ngay cho Trung tâm Thông tin để tổng hợp, báo cáo Lãnh đạo Uỷ ban xem xét, sửa đổi, bổ sung Quy chế cho phù hợp./.

KT.BỘ TRƯỞNG, CHỦ NHIỆM
THỨ TRƯỞNG, PHÓ CHỦ NHIỆM

Phan Văn Hùng