HĐND TỈNH AN GIANG
VĂN PHÒNG

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

Số: 25 /QĐ-VP

An Giang, ngày 11 tháng 9 năm 2018

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng Công nghệ thông tin tại Văn phòng Hội đồng nhân dân tỉnh An Giang

CHÁNH VĂN PHÒNG HỘI ĐỒNG NHÂN DÂN TỈNH AN GIANG

Căn cứ Nghị định số 48/2016/NĐ-CP ngày 27 tháng 5 năm 2016 của Chính phủ quy định cụ thể về chức năng, nhiệm vụ, quyền hạn, cơ cấu tổ chức và biên chế của Văn phòng Hội đồng nhân dân tỉnh, thành phố trực thuộc Trung ương;

Căn cứ Quyết định số 12/QĐ-HĐND ngày 22 tháng 6 năm 2016 của Thường trực Hội đồng nhân dân tỉnh An Giang về việc thành lập Văn phòng Hội đồng nhân dân tỉnh An Giang;

Căn cứ Quyết định số 67/2017/QĐ-UBND ngày 04 tháng 10 năm 2017 của Ủy ban nhân dân tỉnh An Giang ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh An Giang;

Căn cứ Kế hoạch số 179/KH-UBND ngày 01 tháng 8 năm 2018 của Ủy ban nhân dân tỉnh An Giang về thực hiện Chỉ thị số 02/CT-TTg ngày 04/7/2018 của Thủ tướng Chính phủ về công tác bảo vệ bí mật nhà nước trên không gian mạng.

Xét đề nghị của Trưởng phòng Hành chính, Tổ chức, Quản trị,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng Công nghệ thông tin tại Văn phòng Hội đồng nhân dân tỉnh An Giang.

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

Điều 3. Trưởng phòng Hành chính, Tổ chức, Quản trị và cán bộ, công chức, người lao động đang làm việc tại Văn phòng Hội đồng nhân dân tỉnh chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Thường trực HĐND tỉnh;
- Lãnh đạo các Ban HĐND;
- Sở Thông tin và Truyền thông;
- Lưu: VT.

CHÁNH VĂN PHÒNG

VĂN PHÒNG HỘI ĐỒNG NHÂN DÂN TỈNH AN GIANG

Lê Thanh Dũng

HĐND TỈNH AN GIANG
VĂN PHÒNG

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

QUY CHẾ
Bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng Công nghệ thông tin tại Văn phòng Hội đồng nhân dân tỉnh An Giang

(Ban hành kèm theo Quyết định số 25 /QĐ-VP ngày 11 tháng 9 năm 2018 của Chánh Văn phòng Hội đồng nhân dân tỉnh An Giang)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về công tác bảo đảm an toàn thông tin mạng, bao gồm: bảo đảm an ninh, an toàn thông tin mạng; bảo vệ bí mật nhà nước trên không gian mạng; bảo vệ thông tin cá nhân; bảo vệ hệ thống thông tin mạng; đảm bảo an toàn thông tin nội bộ; quản lý và sử dụng thiết bị soạn thảo, lưu trữ văn bản mật trong hoạt động ứng dụng Công nghệ thông tin (CNTT) của Văn phòng Hội đồng nhân dân(HĐND) tỉnh An Giang.

Điều 2. Đối tượng áp dụng

1. Quy chế này áp dụng đối với cơ quan Văn phòng HĐND tỉnh (sau đây gọi tắt là cơ quan).

2. Cán bộ, công chức, người lao động (gọi tắt là cán bộ, công chức) và các cá nhân có liên quan tham gia vận hành, khai thác các hệ thống thông tin tại cơ quan.

3. Doanh nghiệp cung cấp dịch vụ viễn thông, cung cấp dịch vụ phần mềm, cung cấp thiết bị công nghệ thông tin có tham gia vào hoạt động ứng dụng công nghệ thông tin của cơ quan.

Điều 3. Giải thích từ ngữ

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

1. *Mạng nội bộ (LAN - Local Area Networks):* là mạng máy tính được thiết lập bằng cách kết nối các máy tính trong cùng một cơ quan, đơn vị cùng một trụ sở, nhằm chia sẻ tài nguyên, thiết bị dùng chung (như tập tin, máy in, máy quét...);

2. *Mạng diện rộng (WAN) của tỉnh:* là mạng máy tính được thiết lập bằng cách kết nối giữa Trung tâm Tích hợp dữ liệu tỉnh An Giang (Trung tâm Tin học - Sở Thông tin và Truyền thông) với các mạng LAN của các cơ quan, đơn vị thông qua mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;

3. *Mạng truyền số liệu chuyên dùng của các cơ quan Đảng và Nhà nước (MTSLCD):* là mạng truyền dẫn tốc độ cao, sử dụng phương thức chuyển mạch nhãn đa giao thức trên nền giao thức liên mạng (IP/MPLS) sử dụng riêng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan Đảng và Nhà nước do Tập đoàn Bưu chính Viễn thông Việt Nam xây dựng, vận hành;

4. *Mạng Internet:* là mạng máy tính toàn cầu, kết nối tới rất nhiều máy tính và mạng máy tính con trên toàn thế giới;

5. *Ứng cứu sự cố mạng và an toàn thông tin:* Là hoạt động nhằm xử lý, khắc phục sự cố gây mất an toàn thông tin trên hệ thống thông tin;

6. *Cơ sở dữ liệu (database):* là một hệ thống các thông tin có cấu trúc hoặc không cấu trúc được lưu trữ trên các thiết bị lưu trữ thứ cấp (băng từ, đĩa từ...) nhằm thoả mãn yêu cầu khai thác thông tin đồng thời của nhiều người sử dụng hay nhiều chương trình, phần mềm ứng dụng với nhiều mục đích khác nhau;

7. *Phần mềm hệ thống:* là phần mềm dùng để tổ chức và duy trì hoạt động của một hệ thống hoặc một thiết bị số (sau đây gọi chung là thiết bị số). Phần mềm hệ thống có thể tạo môi trường cho các phần mềm ứng dụng làm việc trên đó và luôn ở trạng thái làm việc khi thiết bị số hoạt động.

8. *Phần mềm ứng dụng:* là phần mềm được phát triển và cài đặt trên một môi trường nhất định, nhằm thực hiện những công việc, những tác nghiệp cụ thể.

9. *Máy chủ (Server):* là máy tính được kết nối với hệ thống mạng LAN, WAN hoặc mạng internet, có năng lực xử lý cao, trên đó cài đặt các phần mềm để phục vụ cho các máy tính khác truy cập, yêu cầu cung cấp các dịch vụ hoặc cơ sở dữ liệu.

10. *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. Việc bảo vệ thông tin, tài sản và con người trong hệ thống thông tin nhằm 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. An toàn thông tin bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng.

11. *Phần mềm độc hại* là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay 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.

12. *Hệ thống thông tin:* là một hệ thống bao gồm con người, dữ liệu, các quy trình và công nghệ thông tin tương tác với nhau để thu thập, xử lý, lưu trữ và cung cấp thông tin cần thiết ở đầu ra nhằm hỗ trợ cho một hệ thống.

13. *Người dùng:* cán bộ, công chức của cơ quan sử dụng máy tính, các thiết bị điện tử để xử lý công việc.

Điều 4. Nguyên tắc bảo đảm an toàn thông tin mạng

1. Các cán bộ, công chức và người lao động 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, an ninh 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 các phòng và cá nhân cán bộ, công chức, người lao động.

Chương II
NỘI DUNG BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 5. 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 cơ quan, 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, đầu nối, truy cập trái phép vào các phần mềm dùng chung của cơ quan, 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 cơ quan, tỉnh.

c) Khi khai thác, sử dụng các phần mềm dùng chung của cơ quan, 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. Cơ quan, cá nhân 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) Khi cán bộ, công chức đã nghỉ việc hoặc chuyển công tác, các cơ quan 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 6. Quy định đảm bảo an toàn 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 tuân thủ các điều kiện sau:

- Hệ thống mạng nội bộ (mạng LAN) của cơ quan phải được 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 tại các cơ quan phải được cài đặt các phần mềm bảo vệ, phòng chống vi-rút.

- Các thiết bị CNTT dùng để soạn thảo, in ấn văn bản, lưu trữ thông tin bí mật nhà nước trong cơ quan phải được kiểm định và bố trí riêng, tiến hành ở nơi đảm bảo bí mật, an toàn. Trên máy tính này phải thực hiện các chế độ mã hóa, phân quyền và đặt mật khẩu (password) cho người được giao sử dụng để đảm bảo an toàn, bảo mật thông tin.

- 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.

- 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.

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

- Quản lý các tài khoản của hệ thống thông tin, tài khoản người dùng bao gồm: Tạo mới, sửa đổi, hủy các tài khoản. Thường xuyên kiểm tra các tài khoản của hệ thống thông tin; triển khai các công cụ để hỗ trợ việc quản lý các tài khoản của hệ thống thông tin;

- 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 cá nhân để đảm bảo an toàn thông tin mạng cho các hệ thống thông tin cơ quan đang quản lý, vận hành.

- Định kỳ hàng tuần sao lưu (backup) thông tin (không lưu đè thông tin, sao lưu dự phòng các thông tin thay đổi), dữ liệu của đơn vị và lưu trữ thông tin sao lưu ở nơi an toàn theo quy định; thường xuyên kiểm tra thông tin, dữ liệu sao lưu đảm bảo tính sẵn sàng và toàn vẹn.

2. Kiểm soát và theo dõi tất cả các phương pháp truy cập từ xa tới hệ thống thông tin; phát hiện sớm việc truy cập trái phép vào mạng máy tính hay thiết bị lưu trữ dữ liệu;

3. Thiết lập hệ thống thông tin ghi nhận và lưu vết các sự kiện: Quá trình đăng nhập hệ thống, các thao tác cấu hình hệ thống, quá trình truy xuất hệ thống...

4. 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 thủ trưởng đơn vị;

5. 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.

Điều 7. Quy định bảo vệ bí mật nhà nước trên không gian mạng:

1. Bảo vệ chặt chẽ mọi tài khoản điện tử công vụ (tài khoản quản trị hệ thống mạng, hộp thư điện tử công vụ, tài khoản hệ thống điều hành và quản lý văn bản, tài khoản quản trị Cổng thông tin điện tử). Không sử dụng tài khoản công vụ vào mục đích cá nhân trên Internet.

2. Nghiêm cấm soạn thảo, lưu trữ, sao chụp thông tin bí mật nhà nước trên máy tính hoặc thiết bị nhớ ngoài, phương tiện điện tử có tính năng lưu trữ thông tin có kết nối Internet; kết nối vật lý hệ thống mạng nội bộ chứa thông tin bí mật nhà nước với mạng Internet và ngược lại; trao đổi thông tin bí mật nhà nước qua điện thoại di động, điện thoại cố định, máy fax, hộp thư điện tử công vụ hoặc qua hộp thư điện tử cá nhân, các dịch vụ mạng xã hội trên Internet.

3. Nghiêm cấm chuyển mục đích sử dụng từ máy tính dùng để soạn thảo lưu trữ thông tin có nội dung bí mật nhà nước sang máy tính có kết nối Internet và ngược lại mà chưa có giải pháp hủy dữ liệu triệt để. Trường hợp thiết bị, phương tiện điện tử có lưu trữ nội dung bí mật nhà nước bị hỏng, không có khả năng sửa chữa, phục hồi, không hoạt động được do thiếu đồng bộ, lạc hậu mà không có nhu cầu sử dụng lại phải được bảo quản, xử lý hoặc tiêu hủy theo đúng quy trình, quy định của pháp luật về bảo vệ bí mật nhà nước.

4. Nghiêm cấm sử dụng thiết bị nhớ ngoài USB, ổ cứng di động và các thiết bị, phương tiện điện tử có khả năng lưu trữ dữ liệu khác để sao chép dữ liệu giữa các máy tính soạn thảo nội dung bí mật nhà nước với máy tính hoặc thiết bị, phương tiện điện tử có kết nối Internet.

5. Không sử dụng micro vô tuyến, máy tính, máy tính bảng, điện thoại di động, thiết bị ghi âm, ghi hình, thu phát tín hiệu có khả năng kết nối Internet trong các cuộc họp có nội dung bí mật nhà nước.

6. Kiểm tra, kiểm soát dữ liệu trước khi đăng tải trên cổng thông tin điện tử cơ quan thực hiện theo quy định Danh mục tài liệu, số liệu, thông tin công bố, công khai của các cơ quan hành chính nhà nước các cấp trên địa bàn tỉnh An Giang (Ban hành kèm theo Quyết định số 1135/QĐ-UBND ngày 24 tháng 6 năm 2015 của Ủy ban nhân dân tỉnh An Giang).

Điều 8. 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 vi-rút phù hợp. Các phần mềm phòng chống vi-rút phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc, vi-rút khi sao chép, mở các tập tin.

b) Các 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 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, vi-rút 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 vi-rút, 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 công chức chuyên trách CNTT của cơ quan để xử lý.

Điều 9. Quy định việc truy cập, khai thác, sử dụng mạng Internet

1. Cán bộ, công chức và người lao động không được truy cập, đăng tải, bình luận hoặc sử dụng mạng xã hội để làm việc riêng trong giờ hành chính. Nghiêm cấm việc sử dụng mạng Internet, mạng nội bộ trong giờ hành chính nhằm mục đích cá nhân như: chơi game, xem phim, đăng hình, truy cập các trang web nhạy cảm, các trang web bị cấm, mua bán hàng online, đăng tải phát tán tài liệu cơ quan lên mạng Internet...

2. Cán bộ, công chức và người lao động không được sử dụng, truy cập, khai thác hộp thư công vụ của cơ quan hoặc sử dụng tài khoản hộp thư công vụ cơ quan nhằm mục đích cá nhân. Trừ trường hợp được lãnh đạo cơ quan cho phép sử dụng hoặc những trường hợp cấp thiết. Chỉ văn thư cơ quan, công chức chuyên trách CNTT và lãnh đạo cơ quan mới được phép sử dụng, truy cập và quản lý hộp thư công vụ cơ quan.

3. Cán bộ, công chức và người lao động khi sử dụng hộp thư điện tử tỉnh An Giang phải tuân thủ nghiêm chỉnh Quy chế quản lý và sử dụng hệ thống thư điện tử tỉnh An Giang trong hoạt động của cơ quan nhà nước (Ban hành kèm theo Quyết định số 63/2016/QĐ-UBND ngày 13 tháng 9 năm 2016 của Ủy ban nhân dân tỉnh An Giang).

4. Công chức phụ trách quản trị Cổng thông tin điện tử cơ quan khi đăng tải tin bài, tài liệu, nghị quyết; chỉnh sửa, bổ sung tính năng, giao diện; xóa, gỡ bỏ tin bài, tài liệu, nghị quyết … phải được sự đồng ý của lãnh đạo Ban biên tập Cổng thông tin điện tử cơ quan và thực hiện đúng theo Quy chế quản lý, vận hành, cung cấp thông tin và duy trì hoạt động Cổng thông tin điện tử của cơ quan nhà nước trên địa bàn tỉnh An Giang (Ban hành kèm theo Quyết định số 03/QĐ-UBND ngày 13 tháng 01 năm 2017 của Ủy ban nhân dân tỉnh An Giang).

5. Cán bộ, công chức sử dụng máy vi tính không phải là máy vi tính dự thảo văn bản mật đều được truy cập mạng Internet nhằm mục đích phục vụ công việc cơ quan nhưng phải tuân thủ nghiêm quy chế này và các quy định khác của pháp luật.

Điều 10. Quy định quản lý và sử dụng thiết bị CNTT soạn thảo, lưu trữ văn bản mật

1. Đảm bảo an toàn thông tin văn bản mật:

a) Máy tính soạn thảo văn bản mật: là máy tính không kết nối mạng LAN, WAN, Internet và được kiểm định bảo mật an toàn thông tin (sau đây gọi tắt là máy tính mật).

b) Khi soạn thảo văn bản mật hoặc có tính mật phải sử dụng máy tính mật để soạn thảo.

c) Thiết bị dùng để lưu trữ văn bản mật là ổ cứng (HDD) của máy tính mật hoặc thiết bị lưu trữ di động chỉ được kết nối với máy tính mật, không được kết nối với bất kỳ máy tính, thiết bị nào khác và được kiểm định bảo mật an toàn thông tin.

2. Tiêu hủy thiết bị CNTT soạn thảo, lưu trữ văn bản mật:

a) Xóa văn bản mật: thực hiện thao tác xóa (delete) văn bản mật trên máy tính kể cả trong thùng rác (Recycle Bin).

b) Tiêu hủy ổ cứng trên máy tính mật: Khi máy tính mật hết thời gian khấu hao, ổ cứng có dấu hiệu hư hỏng hoặc đã hư hỏng thì không được tận dụng hoặc sửa chữa để sử dụng vào mục đích khác mà tiến hành tiêu hủy, các bước thực hiện như sau:

Bước 1: Tiến hành sao chép dữ liệu ra thiết bị lưu trữ di động dữ liệu mật để bảo quản (trường hợp còn sử dụng được);

Bước 2: Tháo ổ cứng ra khỏi máy tính mật. Thực hiện niêm phong ổ cứng bằng cách dán giấy niêm phong bao quanh các cổng kết nối, lập biên bản niêm

phong và giao cho lãnh đạo cơ quan bảo quản trong thời gian 06 tháng nhằm mục đích phục vụ công tác điều tra, thanh tra, khiếu nại, tố cáo (nếu có) liên quan đến lưu trữ trong ổ cứng;

Bước 3: Sau thời gian 06 tháng kể từ ngày niêm phong nếu không có trường hợp điều tra, thanh tra, khiếu nại, tố cáo các vấn đề liên quan đến dữ liệu lưu trữ trong ổ cứng thì cơ quan, đơn vị quản lý tiến hành tiêu hủy ổ cứng ở mức độ vật lý có sự giám sát của lãnh đạo cơ quan và lập biên bản tiêu hủy;

c) Tiêu hủy thiết bị lưu trữ di động dữ liệu mật: Khi thiết bị lưu trữ hết thời gian khấu hao, có dấu hiệu hư hỏng hoặc đã hư hỏng thì không được tận dụng hoặc sửa chữa vào mục đích khác mà tiến hành tiêu hủy, các bước thực hiện như điểm b khoản 3 điều này.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 11. Trách nhiệm của cơ quan

1. Tuân thủ và bảo đảm an toàn thông tin trong ứng dụng công nghệ thông tin, đảm bảo an toàn thông tin mạng nội bộ của cơ quan, đơn vị theo hướng dẫn của Sở Thông tin và Truyền thông theo quy định của quy chế này và các quy định khác của pháp luật có liên quan.

2. Tuyên truyền, phổ biến quy chế này và các quy định khác của pháp luật có liên quan về an toàn thông tin trong phạm vi trách nhiệm và quyền hạn của cơ quan.

3. Thủ trưởng cơ quan tạo điều kiện để cán bộ, công chức chuyên trách CNTT được đào tạo, tập huấn nâng cao năng lực công tác về kiến thức an toàn, an ninh thông tin mạng (khi có yêu cầu của Sở Thông tin và Truyền thông);

4. Tổ chức tuyên truyền rông rãi cho cán bộ, công chức và người lao động cơ quan các quy định của pháp luật về bảo vệ bí mật nhà nước để chủ động phòng ngừa, ngăn chặn lộ, lọt bí mật nhà nước, nhất là trên không gian mạng.

5. Hàng năm, xác định các nhiệm vụ bảo đảm an toàn thông tin hệ thống (mở rộng, nâng cấp trang thiết bị; đào tạo, bồi dưỡng kiến thức CNTT, ...), để đề xuất kinh phí đến cơ quan có thẩm quyền hoặc phân bổ kinh phí duy trì hoạt động hệ thống thông tin hiệu quả;

6. Thường xuyên rà soát, kiểm tra toàn bộ dữ liệu để loại bỏ tài liệu bí mật nhà nước đã được đăng tải trên cổng thông tin điện tử, hệ thống thư điện tử, hệ thống thông tin khác có kết nối Internet. Không để xảy ra tình trạng cán bộ, công chức, nhân viên đăng tải, lưu trữ thông tin bí mật nhà nước trên cổng thông tin điện tử, phương tiện điện tử có kết nối Internet, vi phạm pháp luật về bảo vệ bí mật nhà nước.

7. Khi có sự cố hoặc có nguy cơ mất an toàn thông tin phải kịp thời chỉ đạo khắc phục ngay, ưu tiên sử dụng công chức chuyên trách CNTT trong cơ quan, kịp thời báo cho doanh nghiệp cung cấp dịch vụ và thông báo bằng văn bản cho Sở Thông tin và Truyền thông. Trường hợp không khắc phục được thì phối hợp với Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ.

Điều 12. Trách nhiệm của cán bộ, công chức, người lao động trong cơ quan

1. Trách nhiệm của cán bộ, công chức, người lao động trong cơ quan:

- Nghiêm chỉnh thi hành quy chế này và các quy định khác của pháp luật về bảo đảm an toàn, an ninh thông tin.

- Khi phát hiện sự cố ảnh hưởng đến an toàn, an ninh thông tin hoặc có nguy cơ mất an toàn thông tin như: hệ thống hoạt động chậm bất thường, không truy cập được hệ thống ứng dụng, nội dung cổng thông tin điện tử hoặc giao diện ứng dụng bị thay đổi, các sự cố khác có liên quan …, phải thông báo ngay đến công chức chuyên trách CNTT hoặc thông qua phòng Hành chính, Tổ chức, Quản trị của cơ quan để kịp thời khắc phục.

- Khi phát hiện hành vi chiếm đoạt, đánh cắp, lộ, lọt thông tin bí mật nhà nước trên không gian mạng phải kịp thời thông báo ngay đến lãnh đạo cơ quan hoặc thông qua Trưởng phòng Hành chính – Tổ chức – Quản trị để kịp thời khắc phục, xử lý.

- Các thông tin, tài liệu, văn bản có tính mật theo quy định phải dự thảo, lưu trữ đúng theo quy định về bảo mật và an toàn thông tin.

- Không được đăng tải, lưu trữ thông tin bí mật nhà nước trên cổng thông tin điện tử văn phòng, phương tiện điện tử có kết nối Internet, vi phạm pháp luật về bảo vệ bí mật nhà nước.

2. Trách nhiệm của công chức chuyên trách CNTT:

a) Tham mưu triển khai thực hiện các nội dung tại Điều 5, Điều 6 Quy chế này;

b) Theo nhiệm vụ được Thủ trưởng cơ quan phân công, chịu trách nhiệm tham mưu chuyên môn và vận hành đảm bảo an toàn hệ thống thông tin tại cơ quan;

c) Hướng dẫn, hỗ trợ người dùng tại cơ quan giải pháp phòng, chống vi rút máy tính. Thực hiện việc đánh giá, báo cáo các rủi ro và mức độ các rủi ro ảnh hưởng đến hoạt động hệ thống thông tin của đơn vị, các giải pháp cơ bản khắc phục các rủi ro;

d) Phối hợp với các cá nhân, Thường trực, các Ban, các phòng và tổ chức có liên quan trong việc kiểm tra, phát hiện, phòng ngừa, đấu tranh, ngăn chặn xâm phạm an toàn, an ninh thông tin; tham gia khắc phục các sự cố mất an toàn, an ninh thông tin.

CHƯƠNG IV
TỔ CHỨC THỰC HIỆN

Điều 13. Công tác kiểm tra an toàn thông tin

Định kỳ hàng năm tối thiểu 01 lần, tiến hành kiểm tra thường xuyên hoặc đột xuất trang thiết bị CNTT của cán bộ, công chức và người lao động trong cơ quan khi có dấu hiệu vi phạm an toàn an ninh thông tin.

Điều 14. Xử lý vi phạm

Cán bộ, công chức cơ quan có hành vi vi phạm Quy chế này, tùy theo tính chất, mức độ vi phạm mà bị xử lý theo quy định của pháp luật. Xử lý nghiêm, triệt để mọi trường hợp chiếm đoạt, đánh cắp, lộ, lọt thông tin bí mật nhà nước trên không gian mạng theo quy định pháp luật.

Điều 15. Điều khoản thi hành

1. Phòng Hành chính, Tổ chức, Quản trị có trách nhiệm chủ trì, phối hợp với các cơ quan, tổ chức liên quan triển khai và theo dõi việc thực hiện Quy chế này.

2. Định kỳ vào ngày 15/10 hàng năm hoặc đột xuất theo yêu cầu theo yêu cầu về Sở Thông tin và Truyền thông báo cáo kết quả thực hiện quy chế này.

Trong quá trình thực hiện Quy chế này, nếu có vướng mắc đề nghị cán bộ, công chức kịp thời phản ảnh về phòng Hành chính, Tổ chức, Quản trị để tổng hợp, báo cáo Lãnh đạo cơ quan xem xét, sửa đổi, bổ sung Quy chế cho phù hợp./.

CHÁNH VĂN PHÒNG

CỘNG HÒA X.H.C.N VIỆT NAM
VĂN PHÒNG HỘI ĐỒNG NHÂN DÂN
TỈNH AN GIANG

Lê Thanh Dũng