

QUYẾT ĐỊNH

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 trên địa bàn huyện Xuân Lộc

ỦY BAN NHÂN DÂN HUYỆN XUÂN LỘC

Căn cứ Luật Tổ chức Hội đồng nhân dân và Ủy ban nhân dân ngày 26/11/2003;

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

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 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 về Quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng;

Căn cứ Chỉ thị số 15/CT-TTg ngày 17/6/2014 của Thủ tướng Chính phủ về tăng cường công tác đảm bảo an ninh và an toàn thông tin mạng trong tình hình mới;

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;

Căn cứ Quyết định số 02/2014/QĐ-UBND ngày 14/01/2014 của UBND tỉnh Đồng Nai về ban hành quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan quản lý hành chính nhà nước trên địa bàn tỉnh Đồng Nai;

Theo đề nghị của Trưởng phòng Văn hóa và Thông tin tại Tờ trình số 21/TTr.VH&TT ngày 17/6/2015,

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 của cơ quan nhà nước huyện Xuân Lộc.

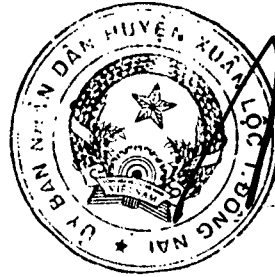
Điều 2. Quyết định này có hiệu lực kể từ ngày ký.

Điều 3: Các cơ quan chuyên môn và đơn vị sự nghiệp, cán bộ, công chức, viên chức và người lao động thuộc Ủy ban dân huyện và Ủy ban dân dân các xã, thị trấn trên địa bàn huyện chịu trách nhiệm thi hành Quyết định này./.

**TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH**

Nơi nhận:

- Như Điều 3;
- UBND tỉnh Đồng Nai;
- Sở Thông tin và Truyền thông;
- Thường trực Huyện ủy;
- Chủ tịch, các PCT.UBND huyện;
- UBMTTQVN và các Đoàn thể huyện;
- Chánh, Phó Văn phòng;
- Cơ quan, đơn vị;
- UBND các xã, thị trấn;
- Lưu: VT, TH(VHTT).



Hồ Văn Hà

QUY CHẾ

**Về đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin
trong hoạt động của các cơ quan nhà nước trên địa bàn
huyện Xuân Lộc**

*(Ban hành kèm theo Quyết định số ~~1586~~ 1586/QĐ-UBND
ngày 22 tháng 7 năm 2015 của Ủy ban nhân dân huyện)*

Chương I

QUY ĐỊNH CHUNG

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

1. Quy chế này quy định về công tác đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước, đơn vị sự nghiệp của huyện Xuân Lộc (sau đây gọi tắt là cơ quan).

2. Quy chế này được áp dụng đối với các các tổ chức, cá nhân liên quan đến an toàn, an ninh thông tin trong các cơ quan nhà nước, đơn vị sự nghiệp của huyện Xuân Lộc.

Điều 2. Mục đích, nguyên tắc đảm bảo an toàn thông tin

1. 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 quá trình ứng dụng công nghệ thông tin trong hoạt động của các cơ quan.

2. Các hoạt động ứng dụng công nghệ thông tin phải tuân theo nguyên tắc đảm bảo an toàn thông tin được quy định tại Điều 41, Nghị định 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước.

Chương II

QUY ĐỊNH ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 3. Về quản lý cán bộ, công chức, viên chức và người lao động

1. Các cơ quan phải xây dựng các yêu cầu, trách nhiệm đảm bảo an toàn thông tin đối với từng vị trí công việc. Trước khi tiếp nhận nhân sự, các cơ quan phải kiểm tra khả năng đáp ứng các yêu cầu về an toàn thông tin của nhân sự mới. Trong các hợp đồng lao động, phải có các điều khoản về trách nhiệm đảm bảo an toàn thông tin.

2. Các cơ quan phải thường xuyên tổ chức quán triệt các quy định về an toàn thông tin nhằm nâng cao nhận thức về trách nhiệm đảm bảo an toàn thông tin của từng cá nhân trong cơ quan.

3. Hủy tài khoản, quyền truy cập các hệ thống thông tin, thu hồi lại tất cả các tài sản liên quan tới hệ thống thông tin (khoá, thẻ nhận dạng, thư mục lưu trữ, thư điện tử, máy vi tính, ...) đối với các cá nhân nghỉ việc, chuyển công tác.

Điều 4. Quản lý phòng máy chủ

1. Các thiết bị mạng quan trọng như tường lửa (firewall), thiết bị định tuyến (router), hệ thống máy chủ, ... phải được đặt trong phòng máy chủ và có các biện pháp bảo vệ, ngăn chặn xâm nhập trái phép vào phòng máy chủ.

2. Phòng máy chủ của các cơ quan là khu vực hạn chế tiếp cận và được lắp đặt hệ thống camera giám sát. Chỉ những người có trách nhiệm theo quy định của thủ trưởng cơ quan mới được phép vào phòng máy chủ.

3. Quá trình vào, ra phòng máy chủ phải được ghi nhận vào nhật ký quản lý phòng máy chủ.

4. Phòng máy chủ phải có hệ thống lưu điện đủ công suất và duy trì thời gian hoạt động của các máy chủ tối thiểu 15 phút khi có sự cố mất điện.

Điều 5. Phòng chống mã độc

1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống mã độc. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin.

2. Các cán bộ, công chức, viên chức và người lao động trong cơ quan phải được hướng dẫn về phòng chống mã độc, 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.

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

4. Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng.

5. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu,...), người sử dụng phải tắt máy và báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý.

6. Các cơ quan, đơn vị phải bố trí máy vi tính riêng, không sử dụng internet để soạn thảo văn bản, lưu trữ thông tin có nội dung mật theo quy định. Không được kết nối đồng thời internet công cộng của các nhà cung cấp dịch vụ internet khác như (XDSL, thiết bị 3G,...) vào mạng truyền số liệu chuyên dùng riêng cho cơ quan Đảng, Nhà nước.

7. Các thiết bị viễn thông, máy tính được sử dụng để lưu giữ và truyền thông tin bí mật nhà nước phải được chứng nhận của Công an tỉnh kiểm tra, kiểm định trước khi đưa vào sử dụng (theo Chỉ thị số 17/CT-UBND ngày 24/5/2013 của Chủ tịch UBND tỉnh).

Điều 6. Sao lưu dữ liệu dự phòng

1. Các dữ liệu quan trọng của cơ quan phải được sao lưu, bao gồm: thông tin cấu hình của hệ thống mạng, máy chủ; phần mềm ứng dụng và cơ sở dữ liệu; tập tin ghi nhật ký.

2. Các cơ quan phải lập kế hoạch và thực hiện sao lưu dữ liệu phù hợp với điều kiện của từng cơ quan, đảm bảo khả năng phục hồi dữ liệu khi có sự cố xảy ra.

3. Khả năng phục hồi dữ liệu phải được kiểm tra định kỳ trên hệ thống và mỗi khi có bất cứ sự thay đổi nào trên hệ thống hoặc tiến trình làm ảnh hưởng đến việc sao lưu dự phòng.

Điều 7. Quản lý thiết bị tường lửa

1. Các hạ tầng công nghệ thông tin phải được trang bị tường lửa để ngăn chặn và phát hiện các xâm nhập trái phép vào mạng nội bộ.

2. Nhật ký hoạt động của thiết bị tường lửa phải được lưu giữ an toàn để phục vụ công tác khảo sát, điều tra khi có sự cố xảy ra.

Điều 8. Quản lý nhật ký

1. Các cơ quan phải thực hiện việc ghi nhật ký (log) trên các thiết bị mạng máy tính, phần mềm ứng dụng, hệ điều hành, cơ sở dữ liệu nhằm đảm bảo các sự kiện quan trọng xảy ra trên hệ thống được ghi nhận và lưu giữ.

2. Các nhật ký này phải được bảo vệ an toàn nhằm phục vụ công tác kiểm tra, phân tích khi cần thiết.

3. Các sự kiện tối thiểu cần phải được ghi nhật ký gồm: quá trình đăng nhập hệ thống; tạo, cập nhật hoặc xóa dữ liệu; các hành vi xem, thiết lập cấu hình hệ thống; việc thiết lập các kết nối bất thường vào và ra hệ thống; thay đổi quyền truy cập hệ thống.

4. Thường xuyên thực hiện việc theo dõi bản ghi nhật ký của hệ thống và các sự kiện khác có liên quan để đánh giá, báo cáo các rủi ro và mức độ nghiêm trọng các rủi ro đó.

Điều 9. Quản lý truy cập

1. Các quy định về quản lý truy cập vào hệ thống thông tin, mạng máy tính, thiết bị, phần mềm ứng dụng của đơn vị phải được quy định chi tiết và tổ chức thực hiện nghiêm túc, phù hợp với các quy định của pháp luật về an toàn thông tin.

2. Mỗi tài khoản truy cập các hệ thống thông tin chỉ được cấp cho một người quản lý và sử dụng.

3. Mỗi cán bộ, công chức, viên chức và người lao động chỉ được phép truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình, có trách nhiệm bảo mật tài khoản truy cập thông tin.

4. Các hệ thống thông tin cần giới hạn số lần đăng nhập sai liên tiếp vào hệ thống. Hệ thống tự động khoá tài khoản trong một khoảng thời gian nhất định trước khi tiếp tục cho đăng nhập nếu liên tục đăng nhập sai vượt quá số lần quy định.

5. Tất cả máy trạm, máy chủ phải được đặt mật khẩu truy cập và thiết lập chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng.

6. Khi thiết lập mạng không dây để kết nối với mạng cục bộ thông qua các điểm truy cập, cần thiết lập các tham số như: Tên, SSID, mật khẩu, cấp phép truy cập đối với địa chỉ vật lý (MAC address), mã hóa dữ liệu và thông báo các thông tin liên quan đến điểm truy cập để cơ quan sử dụng, thường xuyên thay đổi mật khẩu.

7. Mật khẩu đăng nhập vào các hệ thống thông tin phải có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự số và ký tự đặc biệt như !, @, #, \$, %, ...) và phải được thay đổi ít nhất 3 tháng/lần.

Điều 10. Quản lý và khắc phục các sự cố an ninh thông tin

1. Phân loại mức độ nghiêm trọng của các sự cố, bao gồm:

a) Thấp: sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan;

b) Trung bình: sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của đơn vị;

c) Cao: sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và gây ảnh hưởng đến một trong các hoạt động chính của cơ quan;

d) Khẩn cấp: sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của cơ quan.

2. Khi có sự cố hoặc nguy cơ mất an toàn thông tin thì lãnh đạo đơn vị phải chỉ đạo kịp thời để khắc phục và hạn chế thiệt hại, báo cáo bằng văn bản cho UBND huyện và Sở Thông tin và Truyền thông.

3. Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của đơn vị, lãnh đạo đơn vị phải báo cáo ngay cho cơ quan UBND huyện, Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ.

Điều 11. Các hành vi bị nghiêm cấm

1. Tạo ra, cài đặt, phát tán vi rút máy tính, phần mềm độc hại trái pháp luật.

2. Xâm nhập, sửa đổi, xóa bỏ nội dung thông tin của cơ quan, cá nhân khác.

3. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin.

4. Ngăn chặn việc truy cập đến thông tin của cơ quan, cá nhân khác trên môi trường mạng, trù trường hợp pháp luật cho phép.

5. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

6. Hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

Chương III

TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN

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

1. Trách nhiệm của cán bộ, công chức, viên chức phụ trách an toàn thông tin:

a) Chịu trách nhiệm đảm bảo an toàn thông tin của đơn vị;

b) Tham mưu lãnh đạo cơ quan ban hành các quy định, quy trình nội bộ, triển khai các giải pháp kỹ thuật đảm bảo an toàn thông tin;

c) Thực hiện việc giám sát, đánh giá, báo cáo thủ trưởng cơ quan các rủi ro mất an toàn thông tin và mức độ nghiêm trọng của các rủi ro đó;

d) Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn, an ninh thông tin.

2. Trách nhiệm của cán bộ, công chức, viên chức trong các cơ quan, đơn vị:

a) Nghiêm túc chấp hành các quy định, quy chế này và các quy định khác của pháp luật về an toàn thông tin. Chịu trách nhiệm đảm bảo an toàn thông tin trong phạm vi trách nhiệm và quyền hạn được giao;

b) Mỗi cán bộ, công chức, viên chức và người lao động phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp các thiết bị trên máy tính; không được vào các trang web không rõ về nội dung; không tải và cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn; không nhấp chuột vào các đường dẫn lạ không rõ về nội dung;

c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin phải báo cáo ngay với cấp trên và bộ phận chuyên trách công nghệ thông tin để kịp thời ngăn chặn và xử lý;

d) 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.

Điều 13. Trách nhiệm của các cơ quan

1. Thủ trưởng các cơ quan, đơn vị có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước Ủy ban nhân dân huyện trong công tác đảm bảo an toàn thông tin của đơn vị mình.

2. Phân công cán bộ chuyên trách hoặc cán bộ kiêm nhiệm đảm bảo an toàn thông tin của cơ quan, đơn vị; tạo điều kiện để các cán bộ phụ trách an toàn thông tin được học tập, nâng cao trình độ về an toàn thông tin.

3. Xây dựng quy định về đảm bảo an toàn thông tin phù hợp với Quy chế này và các quy định của pháp luật.

4. Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố xảy ra một cách kịp thời, nhanh chóng và đạt hiệu quả.

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

6. Định kỳ hàng quý, năm, các cơ quan lập báo cáo về tình hình an toàn thông tin và gửi UBND huyện (qua Phòng Văn hóa và Thông tin tổng hợp báo cáo UBND huyện).

Điều 14. Trách nhiệm của Phòng Văn hóa và Thông tin

1. Tham mưu Ủy ban nhân dân huyện về công tác hướng dẫn đảm bảo an toàn, an ninh thông tin trên địa bàn huyện.

2. Hàng năm xây dựng kế hoạch triển khai công tác đảm bảo an toàn thông tin phục vụ cho việc vận hành các hệ thống thông tin được Ủy ban nhân dân huyện giao quản lý.

3. Phối hợp với Công an huyện và các cơ quan, đơn vị liên quan tổ chức kiểm tra theo định kỳ hoặc đột xuất; kịp thời phát hiện và xử lý theo quy định của pháp luật đối với các cơ quan, tổ chức, cá nhân có các dấu hiệu, hành vi vi phạm an toàn, an ninh thông tin trên địa bàn huyện.

4. Hướng dẫn, giám sát các cơ quan, đơn vị trên địa bàn huyện thực hiện việc đảm bảo an toàn, an ninh cho hệ thống thông tin theo quy định của Nhà nước.

5. Có trách nhiệm thu thập dữ liệu về các sự cố an ninh, đánh giá mức độ thiệt hại báo cáo cho Sở Thông tin và Truyền thông, Ủy ban nhân dân huyện và các cơ quan, đơn vị có liên quan.

Điều 15. Trách nhiệm của Công an huyện

1. Chủ trì, phối hợp với Phòng Văn hóa và Thông tin, Văn Phòng UBND huyện và các cơ quan, đơn vị liên quan xây dựng kế hoạch và chịu trách nhiệm kiểm soát, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống thông tin gây hại đến an toàn, an ninh thông tin trong cơ quan nhà nước.

2. Phối hợp với các cơ quan chức năng trong trao đổi biện pháp kỹ thuật, kiểm tra, đánh giá nhằm đảm bảo an toàn, an ninh thông tin.

3. Tăng cường công tác phòng ngừa, phát hiện và tuyên truyền, phổ biến pháp luật về xử lý tội phạm trong việc đảm bảo an toàn, an ninh thông tin.

4. Điều tra và xử lý các trường hợp vi phạm pháp luật về an toàn, an ninh thông tin theo thẩm quyền.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 16. Khen thưởng và xử lý vi phạm

1. Hàng năm, Phòng Văn hóa và Thông tin dựa trên các điều tra, báo cáo công tác an toàn, an ninh thông tin của các cơ quan, đơn vị để xác lập bảng xếp hạng an toàn, an ninh thông tin, trên cơ sở đó đề xuất Ủy ban nhân dân huyện xem xét khen thưởng theo quy định hiện hành.

2. Các cơ quan, đơn vị 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 hiện hành.

Điều 17. Thủ trưởng các cơ quan, đơn vị, Chủ tịch Ủy ban nhân dân các xã, thị trấn chịu trách nhiệm tổ chức triển khai thực hiện quy chế tại đơn vị mình.

Điều 18. Phòng Tài chính Kế hoạch phối hợp Phòng Văn hóa và Thông tin bố trí kinh phí thực hiện các nhiệm vụ đảm bảo an toàn thông tin của huyện.

Điều 19. Trong quá trình thực hiện, nếu có những vấn đề cần sửa đổi, bổ sung, đề nghị các cơ quan, đơn vị có ý kiến gửi về Phòng Văn hóa và Thông tin để tổng hợp, báo cáo Ủy ban nhân dân huyện xem xét, quyết định.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH



Hồ Văn Hà