ỦY BAN NHÂN DÂN TỈNH NGHỆ AN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 87/2016/QĐ-UBND	*Nghệ An, ngày 28 tháng 12 năm 2016*

QUYẾT ĐỊNH
Ban hành quy chế đảm bảo an toàn thông tin mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Nghệ An

ỦY BAN NHÂN DÂN TỈNH NGHỆ AN

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19 tháng 6 năm 2015;

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

Căn cứ Luật Viễn thông ngày 23 tháng 11 năm 2009;

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Pháp lệnh bảo vệ bí mật nhà nước số 30/2000/PL-UBTVQH10 ngày 28 tháng 12 năm 2000 của Uỷ ban Thường vụ Quốc hội;

Căn cứ các Nghị định của Chính phủ: số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước; số 90/2008/NĐ-CP ngày 13 tháng 8 năm 2008 về chống thư rác; số 77/2012/NĐ-CP ngày 05 tháng 10 năm 2012 về sửa đổi, bổ sung một số điều của Nghị định số 90/2008/NĐ-CP ngày 13 tháng 8 năm 2008 về chống thư rác; số 72/2013/NĐ-CP ngày 15 tháng 7 năm 2013 về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng;

Căn cứ các Thông tư của Bộ trưởng Bộ Thông tin và Truyền thông: Thông tư số 23/2011/TT-BTTTT ngày 11 tháng 8 năm 2011 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; Thông tư số 27/2011/TT-BTTTT ngày 04 tháng 10 năm 2011 quy định về điều phối các hoạt động ứng cứu sự cố mạng Internet Việt Nam;

Xét đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 1333/TTr-STT&TT, ngày 08 tháng 11 năm 2016,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn thông tin mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Nghệ An.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày 10 tháng 01 năm 2017.

Điều 3. Chánh Văn phòng UBND tỉnh; Giám đốc Sở Thông tin và Truyền thông; Giám đốc các Sở; Thủ trưởng các ban, ngành cấp tỉnh; Chủ tịch UBND các huyện, thành phố, thị xã; Chủ tịch UBND các xã, phường, thị trấn; các doanh nghiệp viễn thông, công nghệ thông tin trên địa bàn tỉnh và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH
Lê Ngọc Hoa

ỦY BAN NHÂN DÂN
TỈNH NGHỆ AN

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

QUY CHẾ
Đảm bảo an toàn thông tin mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Nghệ An

(Ban hành kèm theo Quyết định số 87/2016/QĐ-UBND ngày 28 tháng 12 năm 2016 của Ủy ban nhân dân tỉnh Nghệ An)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về công tác đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin (viết tắt là CNTT) của các cơ quan nhà nước trên địa bàn tỉnh Nghệ An.

Điều 2. Đối tượng áp dụng

1. Các Sở, ban, ngành; UBND các huyện, thành phố, thị xã; các đơn vị sự nghiệp trực thuộc UBND tỉnh; UBND các xã, phường, thị trấn (sau đây gọi tắt là các cơ quan, đơn vị).

2. Các tổ chức, cá nhân, doanh nghiệp có tham gia quản lý, vận hành, khai thác ứng dụng CNTT trong hoạt động các cơ quan Nhà nước của tỉnh Nghệ An.

3. Cán bộ, công chức, viên chức và người lao động đang công tác trong các cơ quan, đơn vị nêu tại Khoản 1 Điều này.

Điều 3. Các nguyên tắc chung về đảm bảo an toàn thông tin mạng

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 CNTT trong hoạt động của các cơ quan, đơn vị.

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

3. Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức.

4. Các tài liệu có nội dung bí mật nhà nước không được truyền trên mạng mà phải được quản lý theo chế độ mật theo quy định pháp luật hiện hành. Trường hợp đặc biệt, cần truyền thông tin mật trên mạng phải được Thủ trưởng cơ quan, đơn vị

cho phép, trước khi truyền thông tin phải được mã hóa theo quy định của Luật Cơ yếu.

5. Nghiêm cấm sử dụng máy tính kết nối Internet và các thiết bị di động thông minh để tạo lập, lưu giữ tài liệu có nội dung mật. Các thiết bị viễn thông, máy tính được sử dụng để lưu giữ và truyền thông tin có nội dung mật phải được chứng nhận của cơ quan chức năng kiểm tra, kiểm định trước khi đưa vào sử dụng.

6. Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác.

7. Thủ trưởng cơ quan, đơn vị phải có phương án tổ chức sao lưu dữ liệu dự phòng cho mọi dữ liệu quan trọng của tỉnh, của cơ quan, đơn vị và chịu trách nhiệm nếu để xảy ra mất mát dữ liệu do không tiến hành sao lưu dự phòng.

8. Để phục vụ hoạt động theo dõi, giám sát, phân tích và điều tra, các cơ quan, đơn vị phải thực hiện việc lưu trữ nhật ký của các hệ thống tại các máy chủ (của hệ điều hành và các phần mềm ứng dụng) trong thời gian ít nhất là 30 ngày.

9. Các thiết bị viễn thông, máy tính có chứa tài liệu của cơ quan nhà nước khi đưa đi công tác nước ngoài phải thực hiện theo quy định của pháp luật về bảo vệ bí mật nhà nước.

10. Hoạt động an toàn thông tin mạng phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.

Chương II

QUY ĐỊNH ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 4. Quản lý gửi thông tin

1. Việc gửi thông tin trên mạng phải bảo đảm các yêu cầu sau đây:

a) Không giả mạo nguồn gốc gửi thông tin;

b) Tuân thủ quy định của Luật An toàn thông tin mạng và quy định khác của pháp luật có liên quan.

2. Các cơ quan, đơn vị sử dụng hộp thư điện tử công vụ với địa chỉ tên miền "nghean.gov.vn" hoặc ".chinhphu.vn" được cấp phát để trao đổi văn bản điện tử khi phối hợp công việc, không sử dụng hộp thư cá nhân (như yahoo, gmail,…).

3. Tổ chức, cá nhân không được gửi thông tin mang tính thương mại, cá nhân vào địa chỉ điện tử của người tiếp nhận khi chưa được người tiếp nhận đồng ý hoặc khi người tiếp nhận đã từ chối, trừ trường hợp người tiếp nhận có nghĩa vụ phải tiếp nhận thông tin theo quy định của pháp luật.

Điều 5. 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, đơn vị là khu vực hạn chế tiếp cận và được được lắp đặt hệ thống camera giám sát. Chỉ những người có trách nhiệm theo quy định của Thủ trưởng cơ quan, đơn vị 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. Cán bộ được giao quản lý phòng máy chủ phải thường xuyên theo dõi, bảo đảm an toàn môi trường vật lý (nhiệt, độ ẩm, ánh sáng,...) cho phòng máy chủ, các hệ thống hỗ trợ (máy điều hòa nhiệt độ, nguồn cấp điện, dự phòng nguồn điện, cáp quang truyền dẫn) được an toàn và hoạt động ổn định, sẵn sàng.

5. Thủ trưởng các cơ quan, đơn vị phải chỉ đạo các bộ phận chức năng có biện pháp bảo vệ đối với phòng máy chủ nhằm phòng, chống nguy cơ do cháy nổ, ngập lụt, động đất và các thảm họa khác do thiên nhiên và con người gây ra.

Điều 6. Phòng chống mã độc, virus

1. Các hệ thống thông tin quan trọng như: Cổng/Trang thông tin điện tử, thư điện tử, quản lý văn bản và điều hành, một cửa điện tử,... phải thường xuyên cập nhật phiên bản mới, bản vá lỗi của các phần mềm nhằm kịp thời phát hiện, loại trừ các mã độc, vi rút máy vi tính.

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

3. Cán bộ, công chức, viên chức và người lao động trong cơ quan, đơn vị phải được hướng dẫn về phòng chống mã độc, các rủi ro do mã độc gây ra;

4. Tất cả các máy tính của cơ quan, 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.

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

6. Khi phát hiện ra bất kỳ dấu hiện 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 cán bộ hoặc bộ phận có trách nhiệm của cơ quan, đơn vị để xử lý.

Điều 7. Sao lưu dữ liệu dự phòng

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

Điều 8. Quản lý thiết bị tường lửa

1. Các hạ tầng CNTT 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 9. Quản lý nhật ký trong quá trình vận hành các hệ thống thông tin

1. Các cơ quan, đơn vị 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. Cán bộ chuyên trách hoặc cán bộ được giao phụ trách CNTT của các cơ quan, đơn vị phải 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 10. 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 cơ quan, 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 triển khai các thiết bị kết nối mạng (như router, switch, camera, wifi,...), phải thiết lập mật khẩu mới thay cho mật khẩu mặc định của thiết bị.

7. Khi thiết lập mạng không dây trong nội bộ cơ quan, đơn vị, phải đặt mật khẩu truy cập vào mạng không dây và chỉ cho phép truy cập Internet.

8. 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 !, @, #, $, %,...). Đối với các hệ thống phần mềm mới được đưa vào sử dụng, phải đổi mật khẩu mặc định của người dùng ngay sau khi được cấp, tiếp nhận tài khoản. Định kỳ phải thay đổi mật khẩu (ít nhất sau 60 ngày đổi một lần), không đặt chế độ ghi nhớ mật khẩu khi sử dụng.

9. Cán bộ chuyên trách hoặc cán bộ được giao phụ trách CNTT của các cơ quan, đơn vị phải thực hiện 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, chữ ký số, máy vi tính, ...) của cơ quan, đơn vị đối với các cá nhân nghỉ việc, chuyển công tác.

Điều 11. Quản lý thiết bị

1. Thiết bị CNTT đặt tại phòng máy chủ của các cơ quan, đơn vị phải đặt tên và dán nhãn theo đúng quy định.

2. Khi sửa chữa các thiết bị CNTT, hạn chế cho phép mang thiết bị, nhất là thiết bị lưu trữ dữ liệu ra khỏi cơ quan, đơn vị và phải bố trí cán bộ giám sát.

3. Khi thanh lý tài sản là thiết bị CNTT như máy trạm, máy chủ,... không thanh lý ổ cứng và các thiết bị lưu trữ dữ liệu mà phải tiêu hủy theo quy định.

Điều 12. Quản lý bản quyền phần mềm

1. Các phần mềm, chương trình ứng dụng sử dụng cho máy chủ tại cơ quan, đơn vị phải có bản quyền sử dụng theo đúng quy định của pháp luật. Khuyến khích sử dụng các phần mềm mã nguồn mở.

2. Cán bộ, công chức, viên chức và người lao động trong các cơ quan, đơn vị không được phát tán, chia sẻ phần mềm có bản quyền đã được đầu tư, cấp phát cho các đối tượng bên ngoài cơ quan, đơn vị với mục đích ngoài nhiệm vụ chuyên môn được giao.

Điều 13. An toàn cho máy tính cá nhân (máy tính để bàn, máy tính xách tay)

1. Cài đặt phần mềm diệt virus, mã độc cho tất cả các máy tính trong mạng LAN của cơ quan, đơn vị, thiết lập chế độ cập nhật hàng ngày cho phần mềm diệt virus.

2. Thủ trưởng các cơ quan, đơn vị phải quán triệt cán bộ, công chức, viên chức và người lao động của cơ quan, đơn vị mình không được cài đặt phần mềm không rõ nguồn gốc, xuất xứ; không truy cập những trang web có nội dung không lành mạnh, không mở những thư điện tử không rõ địa chỉ người gửi,… để tránh tối đa việc các phần mềm virus, mã độc sẽ tự động cài đặt vào máy tính cá nhân.

3. Mã hóa phân vùng ổ cứng chứa dữ liệu quan trọng trên các máy tính cá nhân bằng các phần mềm chuyên dùng (như phần mềm: Bitlocker trên Windows 7,

Windows 8, …).

4. Không chia sẻ thư mục trên mạng LAN theo cơ chế cho phép toàn quyền đọc, ghi (Share Full), chỉ thiết lập cơ chế cho phép chỉ đọc (Read Only) và yêu cầu sử dụng mật khẩu khi truy cập thư mục chia sẻ.

Điều 14. An toàn khi sử dụng các thiết bị lưu trữ ngoài

1. Việc sử dụng các thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB,... phải quét virus trước khi đọc hoặc sao chép dữ liệu.

2. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu.

Điều 15. Soạn thảo văn bản có nội dung thuộc bí mật nhà nước

1. Thủ trưởng cơ quan, đơn vị phải nghiên cứu, xác định độ mật của các văn bản có nội dung thuộc bí mật nhà nước do cơ quan, đơn vị, địa phương ban hành để quản lý theo đúng quy định.

2. Để đảm bảo an toàn khi sử dụng máy tính cho soạn thảo văn bản có nội dung thuộc bí mật nhà nước, các cơ quan, đơn vị cần bố trí 01 (một) máy tính dùng riêng có đặt mật khẩu truy cập và không kết nối với mạng nội bộ (LAN), mạng Internet theo đúng quy định về soạn thảo các văn bản có tính chất Mật.

Điều 16. Quản lý sự cố

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, đơn vị;

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

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

2. Khi có sự cố hoặc nguy cơ mất an toàn thông tin, Thủ trưởng cơ quan, đơn vị phải chỉ đạo kịp thời để khắc phục và hạn chế thiệt hại, báo cáo nhanh (qua điện thoại, thư điện tử công vụ, fax…) và bằng văn bản cho cơ quan cấp trên trực tiếp quản lý, Đội ứng cứu sự cố mạng, máy tính tỉnh Nghệ An 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 cơ quan, đơn vị, Thủ trưởng cơ quan, đơn vị phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ (mẫu báo cáo về sự cố mất an toàn thông tin quy định tại Phụ lục 1 kèm theo Quy chế này).

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 17. Trách nhiệm của Sở Thông tin và Truyền thông

1. Tham mưu Ủy ban nhân dân tỉnh về công tác đảm bảo an toàn thông tin trên địa bàn tỉnh và chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong việc đảm bảo an toàn cho các hệ thống thông tin dùng chung của tỉnh như: Cổng Thông tin điện tử, Thư điện tử, Giao ban điện tử,… và các hệ thống thông tin dùng chung khác.

2. Chịu trách nhiệm xây dựng và trình Ủy ban nhân dân tỉnh hoặc trình Hội đồng nhân dân tỉnh ban hành các cơ chế, chính sách và hướng dẫn, khuyến nghị về đảm bảo an toàn thông tin mạng cho các cơ quan, đơn vị.

3. Tham mưu Ủy ban nhân dân tỉnh hướng dẫn việc sử dụng các thiết bị CNTT để lưu giữ và truyền tải thông tin bí mật nhà nước.

4. Nghiên cứu, tham mưu Ủy ban nhân dân tỉnh xây dựng đội ngũ cán bộ chuyên trách về an toàn thông tin có trình độ đáp ứng yêu cầu theo quy định; tổ chức bộ phận chuyên trách về an toàn thông tin có trách nhiệm đảm bảo an toàn thông tin cho các hệ thống CNTT dùng chung của tỉnh và hỗ trợ các cơ quan, đơn vị trong tỉnh xử lý sự cố an toàn thông tin mạng.

5. Chủ trì, phối hợp Công an tỉnh và các cơ quan, đơn vị có liên quan định kỳ hàng năm tiến hành công tác thanh tra, kiểm tra, đánh giá công tác đảm bảo an toàn thông tin và xử lý các hành vi vi phạm an toàn thông tin mạng tại các cơ quan nhà nước trên địa bàn tỉnh. Tổ chức kiểm tra đột xuất các cơ quan, đơn vị khi có dấu hiệu vi phạm an toàn thông tin mạng.

6. Hàng năm xây dựng kế hoạch, chương trình, dự án, tổng hợp kinh phí để triển khai công tác an toàn thông tin trong hoạt động ứng dụng CNTT của các cơ quan, đơn vị trên địa bàn tỉnh.

7. Thẩm định về an toàn thông tin mạng trong hồ sơ thiết kế hệ thống thông tin trong của các cơ quan, đơn vị trên địa bàn tỉnh.

8. Xây dựng và triển khai các chương trình đào tạo, hội nghị tuyên truyền an toàn thông tin mạng trong công tác quản lý nhà nước trên địa bàn tỉnh.

9. Hướng dẫn cụ thể về nghiệp vụ quản lý vận hành, kỹ thuật đảm bảo an toàn thông tin; đồng thời, hỗ trợ các cơ quan, đơn vị giải quyết sự cố an toàn thông tin mạng khi có yêu cầu.

10. Thiết lập đường dây nóng, bố trí cán bộ thường trực để tiếp nhận các phản ánh của các cơ quan, đơn vị về nguy cơ gây mất an toàn thông tin; phối hợp hướng dẫn, xử lý kịp thời.

11. Thông báo cho các cơ quan, đơn vị biết và có biện pháp phòng ngừa, ngăn

chặn rủi ro an toàn thông tin mạng, các nguy cơ mất an toàn thông tin do virus, phần mềm độc hại, phần mềm gián điệp gây ra.

12. Định kỳ 6 tháng, hàng năm, hoặc đột xuất tổng hợp báo cáo UBND tỉnh về tình hình đảm bảo an toàn thông tin mạng trong các cơ quan Nhà nước tỉnh Nghệ An.

Điều 18. Trách nhiệm của Công an tỉnh

1. Điều tra và xử lý các trường hợp vi phạm an toàn thông tin theo thẩm quyền.

2. Phối hợp Sở Thông tin và Truyền thông kiểm tra công tác an toàn thông tin đối với các cơ quan, đơn vị trên địa bàn tỉnh.

3. Thường xuyên thông báo cho các cơ quan, đơn vị về phương thức, thủ đoạn của các loại tội phạm xâm phạm an toàn thông tin để có biện pháp phòng ngừa, phát hiện, đấu tranh, ngăn chặn.

4. Thực hiện nhiệm vụ bảo vệ an toàn các công trình quan trọng về an ninh quốc gia trên lĩnh vực CNTT.

Điều 19. Trách nhiệm của Sở Tài chính

Phối hợp với Sở Thông tin và Truyền thông tham mưu UBND tỉnh bố trí kinh phí sự nghiệp hàng năm và kinh phí thực hiện các nhiệm vụ đột xuất phục vụ các hoạt động đảm bảo an toàn thông tin mạng trong các cơ quan, đơn vị trên địa bàn tỉnh.

Điều 20. Sở Kế hoạch và Đầu tư

Chủ trì phối hợp với Sở Thông tin và Truyền thông, Sở Tài chính tổng hợp, tham mưu ưu tiên bố trí nguồn vốn ngân sách trong kế hoạch chi đầu tư phát triển hàng năm để thực hiện thanh toán chi phí chuẩn bị đầu tư và thực hiện các dự án đầu tư đảm bảo an toàn thông tin mạng cho các cơ quan, đơn vị trên địa bàn tỉnh.

Điều 21. Trách nhiệm của Đội ứng cứu sự cố mạng, máy tính tỉnh Nghệ An

1. Tham mưu cho Ủy ban nhân dân tỉnh chỉ đạo tổ chức triển khai công tác đảm bảo an toàn an ninh thông tin và ứng cứu sự cố mạng, máy tính đối với các cơ quan, đơn vị trên địa bàn tỉnh.

2. Hỗ trợ các cơ quan, đơn vị trên địa bàn tỉnh trong công tác đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng CNTT và tổ chức ứng cứu các sự cố mạng, máy tính.

3. Là đầu mối của tỉnh, phối hợp với Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT), các đơn vị chức năng có liên quan ngăn chặn, xử lý và khắc phục sự cố mạng, máy tính các cơ quan, đơn vị trên địa bàn tỉnh.

4. Thực hiện trách nhiệm làm đầu mối ứng cứu sự cố của tỉnh trong mạng lưới ứng cứu sự cố mạng, máy tính trên toàn quốc dưới sự điều phối của Trung tâm ứng cứu khẩn cấp máy tính Việt Nam – VNCERT.

Điều 22. Trách nhiệm của các cơ quan, đơn vị

1. Thủ trưởng các cơ quan, đơn vị có trách nhiệm tổ chức quán triệt, nâng cao nhận thức cho cán bộ, công chức, viên chức và người lao động về đảm bảo an toàn thông tin mạng; tổ chức triển khai thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong công tác đảm bảo an toàn thông tin mạng của cơ quan, đơn vị mình.

2. Bảo vệ an toàn thông tin trong mạng nội bộ là trách nhiệm của các cơ quan, đơn vị quản lý mạng nội bộ đó.

3. Trang bị đầy đủ kiến thức bảo mật cơ bản cho cán bộ, công chức, viên chức và người lao động về an toàn thông tin mạng trước khi cho phép truy nhập và sử dụng hệ thống thông tin. Bố trí, tạo điều kiện làm việc phù hợp với chuyên môn và ưu tiên bồi dưỡng nghiệp vụ về an toàn thông tin mạng cho cán bộ chuyên trách (hoặc cán bộ được giao phụ trách) về CNTT trong các cơ quan, đơn vị. Khuyến khích các cơ quan, đơn vị liên kết với tổ chức, cá nhân, doanh nghiệp CNTT uy tín mở các khóa đào tạo nhân lực trong lĩnh vực an toàn thông tin mạng.

4. Bố trí kinh phí cho việc mua sắm, nâng cấp các trang thiết bị phần cứng, phần mềm để đảm bảo và tăng cường an toàn thông tin trong hoạt động ứng dụng CNTT của cơ quan, đơn vị.

5. Khi có sự cố an toàn thông tin mạng hoặc có nguy cơ mất an toàn thông tin phải kịp thời chỉ đạo khắc phục ngay, ưu tiên sử dụng cán bộ kỹ thuật chuyên trách trong cơ quan, đơn vị. Kịp thời báo cho doanh nghiệp cung cấp dịch vụ và thông báo bằng văn bản cho Đội ứng cứu sự cố mạng, máy tính tỉnh Nghệ An, Sở Thông tin và Truyền thông, cơ quan cấp trên quản lý trực tiếp biết (theo mẫu báo cáo sự cố tại Phụ lục 01 kèm theo Quy chế này). Trường hợp không tự khắc phục được thì phối hợp với Đội ứng cứu sự cố tỉnh Nghệ An, Sở Thông tin và Truyền thông hoặc cơ quan quản lý cấp trên để được hướng dẫn, hỗ trợ xử lý.

6. Xây dựng quy chế nội bộ về đảm bảo an toàn thông tin trong cơ quan, đơn vị mình.

7. Khi triển khai đầu tư ứng dụng CNTT phải có phương án đảm bảo an toàn thông tin từ khâu thiết kế và phải tự chịu trách nhiệm đảm bảo an toàn thông tin cho hệ thống CNTT và các hệ thống thông tin của cơ quan, đơn vị mình.

8. 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 thông tin.

9. Phối hợp với Sở Thông tin và Truyền thông và các cơ quan, đơn vị liên quan thực hiện công tác kiểm tra khắc phục sự cố an toàn thông tin mạng; đồng thời cung cấp đầy đủ các thông tin khi đoàn kiểm tra yêu cầu. Không được che dấu thông tin về sự cố nhằm gây khó khăn cho các cơ quan chức năng đánh giá thiệt hại để có phương án xử lý.

10. Báo cáo tình hình và kết quả thực hiện công tác đảm bảo an toàn thông

tin tại cơ quan, đơn vị, định kỳ hàng năm (trước ngày 15/11) gửi về Sở Thông tin và Truyền thông.

Điều 23. Trách nhiệm của các doanh nghiệp viễn thông, CNTT cung cấp hạ tầng phục vụ ứng dụng CNTT trong cơ quan nhà nước

1. Có trách nhiệm đầu tư, phát triển hạ tầng viễn thông, đường truyền phục vụ việc ứng dụng CNTT đảm bảo an toàn thông tin cho hệ thống do doanh nghiệp thiết lập.

2. Viễn thông Nghệ An có trách nhiệm đảm bảo hệ thống mạng truyền số liệu chuyên dùng của các cơ quan, đơn vị trên địa bàn tỉnh; phối hợp với Cục Bưu điện Trung ương, Sở Thông tin và Truyền thông trong việc xử lý khắc phục khi có sự cố trên hệ thống mạng truyền số liệu chuyên dùng của tỉnh.

Điều 24. Trách nhiệm của các tổ chức, cá nhân, doanh nghiệp có tham gia quản lý, vận hành, khai thác ứng dụng CNTT trong hoạt động các cơ quan Nhà nước của tỉnh Nghệ An

1. Tuân thủ theo quy định tại Quy chế này và các quy định khác của pháp luật có liên quan.

2. Thực hiện tốt các biện pháp đảm bảo an toàn thông tin khi tương tác sử dụng ứng dụng CNTT của các cơ quan Nhà nước phục vụ người dân và doanh nghiệp.

3. Chịu trách nhiệm về các thông tin cá nhân đăng ký, khai báo khi sử dụng tương tác các ứng dụng CNTT của tỉnh; tuân thủ các hướng dẫn khi sử dụng dịch vụ CNTT của tỉnh.

4. Không thu thập, sử dụng, phát tán, quảng cáo, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống dịch vụ ứng dụng CNTT thông tin để thu thập, khai thác thông tin cá nhân.

Điều 25. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các cơ quan, đơn vị

1. Trách nhiệm của cán bộ chuyên trách hoặc cán bộ được giao phụ trách CNTT trong các cơ quan, đơn vị:

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

b) Chịu trách nhiệm triển khai các biện pháp quản lý, vận hành, quản lý kỹ thuật, tham mưu xây dựng quy định về đảm bảo an toàn cho hệ thống thông tin của cơ quan, đơn vị mình theo Quy chế này;

c) Thực hiện việc giám sát, đánh giá, báo cáo Thủ trưởng cơ quan, đơn vị 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, các cơ quan, đơn vị có liên quan trong việc kiểm tra, phát hiện và khắc phục các sự cố mất an toàn thông tin mạng;

2. Trách nhiệm của cán bộ, công chức, viên chức và người lao động:

a) Chấp hành nghiêm túc các quy định 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 toàn thông tin tại cơ quan, đơn vị;

b) Khi phát hiện sự cố mất an toàn thông tin phải báo ngay với cấp trên và bộ phận chuyên trách của cơ quan, đơn vị để kịp thời ngăn chặn, xử lý. Không tự ý liên hệ với cá nhân bên ngoài vào can thiệp các thiết bị phần cứng, phần mềm của cơ quan, đơn vị mình;

c) Không sử dụng hòm thư công vụ (có địa chỉ tên miền "nghean.gov.vn" hoặc "chinhphu.vn") được cấp phát cho cá nhân hoặc cơ quan, đơn vị mình vào mục đích cá nhân như đăng ký tài khoản mạng xã hội, đăng ký mua sắm qua mạng,…

Chương IV

TỔ CHỨC THỰC HIỆN

Điều 26. Khen thưởng và xử lý vi phạm

1. Hàng năm, Sở Thông tin và Truyền thông dựa trên các điều tra, báo cáo công tác an toàn thông tin của các cơ quan, đơn vị đưa an toàn thông tin mạng vào tiêu chí đánh giá xếp hạng ứng dụng CNTT của các cơ quan nhà nước trên địa bàn tỉnh, trên cơ sở đó đề xuất UBND tỉnh xem xét khen thưởng theo quy định.

2. Các cơ quan, đơn vị; cá nhân; Người dân và doanh nghiệp khi vi phạm quy định của Quy chế này, tùy theo tính chất, mức độ vi phạm mà bị xử phạt vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự, nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật.

Điều 27. Điều khoản thi hành

Trong quá trình thực hiện, nếu có vướng mắc, phát sinh, các cơ quan, đơn vị kịp thời phản ánh về Sở Thông tin và Truyền thông để tổng hợp, báo cáo UBND tỉnh xem xét sửa đổi, bổ sung Quy chế cho phù hợp./.

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH
Lê Ngọc Hoa

PHỤ LỤC 01: MẪU BÁO CÁO KHI CÓ SỰ CỐ

(Ban hành kèm theo Quyết định số 87/2016/QĐ-UBND ngày 28 tháng 12 năm 2016 của Ủy ban nhân dân tỉnh Nghệ An)

..... **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**

..... **Độc lập - Tự do - Hạnh phúc**

Nghệ An, ngày ..... tháng ..... năm .....

BÁO CÁO SỰ CỐ

Thông tin chung

▪Tên cơ quan/đơn vị thông báo sự cố * .....

▪Email * .....

▪Điện thoại * .....

Thông tin về sự cố

▪Mô tả sơ bộ về sự cố * .....

.....

▪Cách thức phát hiện * (*Đánh dấu những cách thức được sử dụng để phát hiện sự cố)*

☐ Qua hệ thống phát hiện xâm nhập

☐ Kiểm tra dữ liệu lưu lại (Log File)

☐ Nhận được thông báo từ: .....

☐ Khác, đó là .....

▪Thời gian xảy ra sự cố *: …/… /…/…/… (ngày/tháng/năm/giờ/phút)

(Lưu ý: Ngày, Tháng điền đủ 2 chữ số, Năm điền đủ 4 chữ số, Giờ, Phút điền đủ 2 chữ số theo hệ 24 giờ).

▪Thời gian thực hiện báo cáo sự cố *:…/…/…/…/… (ngày/tháng/năm/giờ/phút)

Đã gửi thông báo sự cố cho *

☐ Thành viên mạng lưới chịu trách nhiệm ứng cứu sự cố cho tổ chức, cá nhân

☐ ISP đang trực tiếp cung cấp dịch vụ

☐ Cơ quan điều phối

Thông tin về hệ thống xảy ra sự cố

a) Tên máy chủ 1 .....

▪Hệ điều hành ..... Version .....

▪Các dịch vụ có trên hệ thống (*Đánh dấu những dịch vụ được sử dụng trên hệ thống)*

☐ Web server ☐ Mail server ☐ Database server

☐ Dịch vụ khác, đó là .....

▪Các biện pháp an toàn thông tin đã triển khai (*Đánh dấu những biện pháp đã triển khai)*

☐ Antivirus ☐ Firewall ☐ Hệ thống phát hiện xâm nhập

☐ Khác:.....

▪Các địa chỉ IP của hệ thống *(Liệt kê địa chỉ IP sử dụng trên Internet, không liệt kê địa chỉ IP nội bộ)*

.....

▪Các tên miền của hệ thống

.....

▪Mục đích chính sử dụng hệ thống .....

.....

▪Thông tin gửi kèm

☐ Nhật ký hệ thống

☐ Mẫu virus / mã độc

☐ Khác:…….

▪Các thông tin cung cấp trong thông báo sự cố này đều phải được giữ bí mật:

☐ Có

☐ Không

▪Sự cố đã được khắc phục:

☐ Đã khắc phục

☐ Chưa khắc phục (đề nghị ứng cứu)

▪Kiến nghị .....

b) Tên máy chủ 2 .....

(Tương tự như mục a - Nếu có)

Tổ chức thông báo

(*ký tên, đóng dấu*)

Chú thích:

1. Phần (*) là những thông tin bắt buộc. Các phần còn lại có thể loại bỏ nếu không có thông tin.

2. Sử dụng tiêu đề (subject) bắt đầu bằng "[TBSC]" khi gửi thông báo qua email