ỦY BAN NHÂN DÂN TỈNH NINH BÌNH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 15 /2016/QĐ-UBND	*Ninh Bình, ngày 06 tháng 7 năm 2016*

QUYẾT ĐỊNH

Ban hành Quy chế đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của các cơ quan nhà nước thuộc phạm vi quản lý của tỉnh Ninh Bình

ỦY BAN NHÂN DÂN TỈNH NINH BÌNH

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

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

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

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước; Nghị định số 72/2013/NĐ-CP ngày 15/07/2013 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;

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 390/TTr-STTTT ngày 30/6/2016 và Báo cáo thẩm định số 77/BC-STP ngày 18/5/2016 của Sở Tư pháp,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực Công nghệ thông tin trong hoạt động của các cơ quan nhà nước thuộc phạm vi quản lý của tỉnh Ninh Bình.

Điều 2. Quyết định này có hiệu lực thi hành sau 10 ngày kể từ ngày ký.

Điều 3. Chánh Văn phòng UBND tỉnh, Giám đốc Sở Thông tin và Truyền thông; Thủ trưởng các Sở, ban, ngành của tỉnh; Chủ tịch UBND các huyện, thành phố và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ Thông tin và Truyền thông (Vụ Pháp chế);
- Bộ Tư pháp (Cục KTVBQPPL);
- Thường trực TU; Thường trực HĐND tỉnh;
- Đoàn Đại biểu Quốc hội tỉnh; UBMTTQ tỉnh;
- Chủ tịch, các Phó Chủ tịch UBND tỉnh;
- Trung tâm TH&CB, Cổng TTĐT tỉnh;
- Lưu: VT, VP6.

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Tống Quang Thìn

ỦY BAN NHÂN DÂN TỈNH NINH BÌNH	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY CHẾ
Đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của các cơ quan nhà nước thuộc phạm vi quản lý của tỉnh Ninh Bình

(Ban hành kèm theo Quyết định số: 15 /2016/QĐ-UBND ngày ..06.tháng 7 năm 2016 của Ủy ban nhân dân tỉnh Ninh Bình)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về công tác đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin (CNTT) trong hoạt động của các cơ quan nhà nước thuộc phạm vi quản lý của tỉnh Ninh Bình (sau đây gọi tắt là cơ quan).

Điều 2. Đối tượng áp dụng

Quy chế này áp dụng đối với cơ quan nhà nước thuộc phạm vi quản lý của tỉnh Ninh Bình và tổ chức, cá nhân khác có liên quan.

Điều 3. Giải thích từ ngữ

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

1. *An toàn thông tin mạng* là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính toàn vẹn, tính bảo mật và tính khả dụng của thông tin.

2. *Mạng* là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính.

3. *Hệ thống thông tin* là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng.

4. *Xâm phạm an toàn thông tin mạng* là hành vi truy nhập, sử dụng, tiết lộ, làm gián đoạn, sửa đổi, phá hoại trái phép thông tin, hệ thống thông tin.

5. *Sự cố an toàn thông tin mạng* là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

6. *Phần mềm độc hại* là phần mềm có tính năng gây hại 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.

7. *Thông tin cá nhân* là thông tin gắn với việc xác định danh tính của một người cụ thể.

8. *Xử lý thông tin cá nhân* là việc thực hiện một hoặc một số thao tác thu thập, biên tập, sử dụng, lưu trữ, cung cấp, chia sẻ, phát tán thông tin cá nhân trên mạng nhằm mục đích thương mại.

9. *Sản phẩm an toàn thông tin mạng* là phần cứng, phần mềm có chức năng bảo vệ thông tin, hệ thống thông tin.

10. *Dịch vụ an toàn thông tin mạng* là dịch vụ bảo vệ thông tin, hệ thống thông tin.

Chương II
ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 4. Quản lý vận hành trong công tác đảm bảo an toàn, an ninh thông tin

1. Đối với các cơ quan, đơn vị:

a) Trang bị đầy đủ các kiến thức bảo mật cơ bản cho cán bộ, công chức, viên chức trước khi cho phép truy nhập và sử dụng hệ thống thông tin.

b) Bố trí cán bộ chuyên trách về an toàn hệ thống thông tin (sau đây gọi tắt là cán bộ chuyên trách). Cán bộ chuyên trách được đảm bảo điều kiện học tập, tiếp cận công nghệ, kiến thức an toàn bảo mật thông tin trước khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ.

c) Quan tâm và ưu tiên bố trí kinh phí cần thiết để đảm bảo và tăng cường an toàn, an ninh thông tin trong hoạt động ứng dụng CNTT của cơ quan, đơn vị.

d) Các cơ quan, đơn vị phải bố trí máy vi tính riêng, không kết nối mạng nội bộ và Internet dùng để soạn thảo văn bản, lưu giữ thông tin có nội dung mật theo quy định.

2. Đối với cán bộ chuyên trách tại các cơ quan, đơn vị:

a) Tham mưu cho lãnh đạo triển khai thực hiện các biện pháp để đảm bảo an toàn, an ninh hệ thống thông tin của cơ quan, đơn vị. Thường xuyên nghiên cứu, cập nhật các kiến thức về an toàn, an ninh thông tin, có biện pháp phòng tránh các nguy cơ tiềm ẩn có thể gây mất thông tin khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ.

b) Thường xuyên cập nhật cấu hình chuẩn cho các thành phần của hệ thống thông tin, thiết lập cấu hình chặt chẽ nhất nhưng vẫn đảm bảo duy trì hoạt động thường xuyên của hệ thống thông tin.

c) Khi thiết lập cấu hình hệ thống thông tin chỉ cung cấp những chức năng thiết yếu nhất; xác định các chức năng, cổng giao tiếp mạng, giao thức, và dịch vụ không cần thiết để cấm hoặc hạn chế sử dụng.

d) Thường xuyên thực hiện việc theo dõi bản ghi nhật ký 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. Các rủi ro đó có thể xảy ra do sự truy cập trái phép, sử dụng trái phép, mất, thay đổi hoặc phá hủy thông tin và hệ thống thông tin.

e) Kiểm soát chặt chẽ cài đặt phần mềm vào máy trạm và máy chủ.

3. Đối với cán bộ, công chức, viên chức:

a) Thường xuyên cập nhật những chính sách, thủ tục an toàn thông tin của cơ quan, đơn vị và thực hiện đúng hướng dẫn về an toàn, an ninh thông tin của cán bộ chuyên trách.

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

c) Các máy tính khi không sử dụng trong thời gian dài (quá 4 giờ làm việc) cần tắt máy hoặc ngưng kết nối mạng, để tránh bị các tin tặc lợi dụng, sử dụng chức năng điều khiển từ xa dùng máy tính của mình tấn công vào các hệ thống thông tin khác.

d) Phải thực hiện quét virus trước khi mở các tập tin đính kèm theo thư điện tử, không mở các thư điện tử khi chưa rõ người gửi hoặc tập tin đính kèm có nguồn gốc không rõ ràng để tránh virus, phần mềm gián điệp lây nhiễm máy tính.

e) Phải đặt mật khẩu cho máy tính (mật khẩu đăng nhập, mật khẩu bảo vệ màn hình). Sử dụng các thiết bị lưu trữ thông tin (USB, ổ cứng gắn ngoài, thẻ nhớ) đảm bảo an toàn, đúng cách để phòng ngừa virus, phần mềm gián điệp xâm nhập máy tính phá hoại, đánh cắp thông tin.

Điều 5. Quản lý phòng máy chủ

1. Hệ thống 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 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 6. Phòng chống mã độc, virus

1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống mã độc, virus. 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.

Điều 7. Sao lưu dữ liệu dự phòng

1. 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. Cơ quan, đơn vị 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.

Điều 8. Quản lý thiết bị tường lửa

1. Hệ thống 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 9. Quản lý nhật ký trong quá trình vận hành các hệ thống thông tin

1. 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, đồng thời các nhật ký này phải được bảo vệ an toàn nhằm phục vụ công tác kiểm tra, phân tích khi cần thiết.

2. Các nội dung 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.

3. Thường xuyên thực hiện việc theo dõi bản ghi nhật ký của hệ thống và các nội dung 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. 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. 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 trong nội bộ đơn vị, phải đặt mật khẩu truy cập vào mạng không dây và chỉ cho phép truy cập Internet.

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 11. 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;

b) Trung bình: Sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoán 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 cơ quan cấp trên trực tiếp quản lý 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 cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ.

Điều 12. Các hành vi bị nghiêm cấm

1. Tạo, cài đặt, phát tán thư rác, tin nhắn rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo; lợi dụng mạng để truyền bá tư tưởng độc hại, đồi trụy, kích động chống phá các chủ trương, đường lối của Đảng, chính sách pháp luật của Nhà nước và các hành vi nghiêm cấm khác theo các quy định của 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 nhập đến thông tin của cơ quan, cá nhân khác trên môi trường mạng, trừ 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, lộ, lọt và phát tán 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, AN NINH THÔNG TIN

Điều 13. Trách nhiệm của các cơ quan, đơn vị

1. Thủ trưởng các cơ quan có trách nhiệm tuyên truyền, nâng cao nhận thức cho cán bộ công chức, viên chức (CBCCVC)về các nguy cơ mất an toàn, an ninh thông tin; tổ chức triển khai đầy đủ các nội dung 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 của đơn vị mình.

2. Khi có sự cố hoặc 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 và thông báo bằng văn bản cho Sở Thông tin và Truyền thông, cơ quan cấp trên quản lý trực tiếp biết. Trường hợp không khắc phục được thì phối hợp với Sở Thông tin và Truyền thông hoặc cơ quan cấp trên quản lý để được hướng dẫn, hỗ trợ.

3. Hủy bỏ quyền truy cập vào hệ thống thông tin, thu hồi lại các tài liệu, hồ sơ, thông tin liên quan tới tài khoản của CBCCVC chuyển công tác, nghỉ hưu hoặc chấm dứt hợp đồng.

4. Thường xuyên tổ chức thực hiện tự kiểm tra, rà soát, phân tích, đánh giá, báo cáo rủi ro và nguy cơ gây mất an toàn, an ninh thông tin đối với hệ thống thông tin của đơn vị.

5. Phối hợp với Sở Thông tin và Truyền thông và các đơn vị có liên quan trong công tác xây dựng, bảo trì, nâng cấp hệ thống bảo đảm an toàn, an ninh thông tin của đơn vị.

6. Áp dụng mọi biện pháp để khắc phục và hạn chế thiệt hai do sự cố xảy ra, lập biên bản báo cáo cho cơ quan cấp trên quản lý trực tiếp, đồng thời thông báo bằng văn bản cho Sở Thông tin và Truyền thông. Trường hợp có sự cố nghiêm trọng vượt quá khả năng khắc phục của đơn vị, phải báo cáo ngay cho Sở Thông tin và Truyền thông và cơ quan quản lý nhà nước cấp trên.

7. Xây dựng quy chế nội bộ về đảm bảo an toàn, an ninh thông tin phù hợp với Quy chế này và các quy định của pháp luật.

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

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

10. Báo cáo tình hình và kết quả thực hiện công tác đảm bảo an toàn, an ninh thông tin tại cơ quan, đơn vị và gửi về Sở Thông tin và Truyền thông định kỳ hàng năm (trước ngày 20 tháng 12).

Điều 14. 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:

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;

e) Thường xuyên cập nhật, nâng cao kiến thức, trình độ chuyên môn đáp ứng yêu cầu đảm bảo an toàn thông tin của đơn vị.

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

a) Nghiêm túc chấp hành các quy định, quy trình nội bộ, Quy chế này và các quy định khác của pháp luật về an toàn, an ninh thông tin. Chịu trách nhiệm bảo mật thông tin và 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 truy cập 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 của cơ quan 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 cơ quan có thẩm quyền tổ chức.

Điều 15. Trách nhiệm của Sở Thông tin và Truyền thông

1. Tham mưu cho Ủy ban nhân dân tỉnh về công tác đảm bảo an toàn, an ninh thông tin trên địa bàn tỉnh và chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong việc đảm bảo an toàn an ninh cho các hệ thống thông tin của tỉnh.

2. Hằng năm triển khai công tác đảm bảo an toàn, an ninh thông tin phục vụ cho việc vận hành các hệ thống thông tin được Ủy ban nhân dân tỉnh giao quản lý.

3. Hằng năm xây dựng và triển khai các chương trình tập huấn về an toàn, an ninh thông tin cho lực lượng đảm bảo an toàn, an ninh thông tin của các cơ quan.

4. Tổ chức các hội nghị, hội thảo chuyên đề và tuyên truyền về an toàn, an ninh thông tin trong công tác quản lý Nhà nước trên địa bàn tỉnh.

5. Tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin.

6. Hướng dẫn, giám sát các cơ quan, đơn vị trên địa bàn tỉnh xây dựng quy chế nội bộ và thực hiện việc đảm bảo an toàn, an ninh cho hệ thống thông tin theo quy định của Nhà nước.

7. Thường xuyên cập nhật các nguy cơ gây mất an toàn, an ninh thông tin và thông báo cho các cơ quan, đơn vị biết để có biện pháp phòng ngừa, ngăn chặn, xử lý kịp thời.

8. 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 mất an toàn, an ninh thông tin.

9. Phối hợp với Ban cơ yếu Chính phủ tổ chức triển khai ứng dụng chữ ký số cho các cơ quan nhà nước của tỉnh; hướng dẫn, khuyến khích các tổ chức, doanh nghiệp và người dân trên địa bàn tỉnh tăng cường ứng dụng chữ ký số trong giao dịch điện tử.

10. Tổng hợp và báo cáo về tình hình an toàn, an ninh thông tin theo quy định.

Điều 16. Trách nhiệm của Công an tỉnh

1. Chủ trì, phối hợp với Sở Thông tin và Truyền thông và các cơ quan, đơn vị có liên quan triển khai công tác đảm bảo an toàn, an ninh thông tin, 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 Sở Thông tin và Truyền thông, các cơ quan chức năng trao đổi biện pháp kỹ thuật nhằm kiểm tra đánh giá công tác đảm bảo an toàn, an ninh thông tin.

3. Điều tra, làm rõ các trường hợp vi phạm an toàn, an ninh thông tin và xử lý theo đúng quy định của pháp luật.

Điều 17. Trách nhiệm của Sở Tài chính

Chủ trì phối hợp với Sở Kế hoạch và Đầu tư, Sở Tài chính phối hợp Sở Thông tin và Truyền thông ưu tiên bố trí kinh phí thực hiện các nhiệm vụ đảm bảo an toàn thông tin tại các đơn vị nêu tại Khoản 1 Điều 2 Quy chế này.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 18. Khen thưởng và xử lý vi phạm

1. Hằng năm, Sở Thông tin và Truyền thông 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 tỉnh xem xét khen thưởng theo quy định hiện hành.

2. Các cơ quan, đơn vị, cá nhân 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 19. Triển khai tổ chức thực hiện Quy chế và sửa đổi, bổ sung Quy chế

1. Sở Thông tin và Truyền thông có trách nhiệm chủ trì phối hợp với các cơ quan có liên quan hướng dẫn triển khai thực hiện Quy chế này.

2. Trong quá trình thực hiện Quy chế, 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 Ủy ban nhân dân tỉnh xem xét sửa đổi, bổ sung cho phù hợp./.

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Tống Quang Thìn