ỦY BAN NHÂN DÂN TỈNH HẢI DƯƠNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 29 /2013/QĐ-UBND	*Hải Dương, ngày 11 tháng 12 năm 2013*

QUYẾT ĐỊNH

Về việc Ban hành Quy chế bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Hải Dương

ỦY BAN NHÂN DÂN TỈNH HẢI DƯƠNG

Căn cứ Luật Tổ chức HĐND và UBND ngày 26 tháng 11 năm 2003;

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

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

Căn cứ Nghị định số 72/2013/NĐ-CP ngày 15 tháng 7 năm 2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng;

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

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 787/TTr-STTTT ngày 25/11/2013,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Hải Dương.

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; Giám đốc các Sở, Ban, Ngành tỉnh; Chủ tịch UBND các huyện, thị xã, 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;
- Cục Kiểm tra văn bản Bộ Tư pháp;
- Thường trực Tỉnh ủy, HĐND&Đoàn ĐBQH tỉnh;
- Chủ tịch, các PCT UBND tỉnh;
- Văn phòng Tỉnh ủy;
- Lãnh đạo VP UBND tỉnh
- Trung tâm Công báo tỉnh;
- Cổng thông tin điện tử tỉnh;
- Lưu: VT. (80)Nam

TM. UỶ BAN NHÂN DÂN TỈNH
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Nguyễn Dương Thái

LawSoft * Tel: +84-8-3930 3279 * www.ThuVienPhapLuat.vn

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

QUY CHẾ

Bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Hải Dương

(Ban hành kèm theo Quyết định số 29 /2013/QĐ-UBND ngày 11 tháng 12 năm 2013 của Ủy ban nhân dân tỉnh Hải Dương)

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 bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh (sau đây gọi tắt là bảo đảm an toàn, an ninh thông tin); trách nhiệm của các cơ quan, đơn vị, cán bộ, công chức, viên chức trong việc bảo đảm an toàn, an ninh thông tin.

2. Quy chế này áp dụng đối với các Sở, Ban, Ngành, Ủy ban nhân dân các huyện, thị xã, thành phố thuộc tỉnh (sau đây gọi chung là các cơ quan, đơn vị) và cán bộ, công chức, viên chức trong các cơ quan, đơn vị. Đối với lực lượng vũ trang tỉnh, ngoài việc thực hiện theo quy định trong Quy chế này còn thực hiện theo quy định riêng của ngành trong việc bảo đảm an toàn, an ninh thông tin.

Điều 2. Giải thích từ ngữ

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

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

2. *An ninh thông tin*: Là việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

3. *Hệ thống thông tin*: Là một tập hợp các thiết bị viễn thông, công nghệ thông tin bao gồm phần cứng, phần mềm (Cổng/trang thông tin điện tử, hệ thống thư điện tử, phần mềm quản lý văn bản và hồ sơ công việc, hệ thống giao ban trực tuyến, phần mềm dịch vụ công trực tuyến,...) và cơ sở dữ liệu phục vụ cho hoạt động lưu trữ, xử lý, truyền đưa, chia sẻ, trao đổi, cung cấp và sử dụng thông tin.

4. *Mạng riêng ảo*: Là một mạng dành riêng sử dụng hệ thống mạng công cộng (thường là Internet) để kết nối các máy tính ở xa lại với nhau. Nó được thiết lập để cho phép các máy tính gửi và nhận dữ liệu với tất cả các chức năng, chính sách quản lý và bảo mật của mạng nội bộ.

LawSoft * Tel: +84-8-3930 3279 * www.ThuVienPhapLuat.vn

5. *Cổng giao tiếp*: Để định danh các ứng dụng gửi và nhận dữ liệu, mỗi ứng dụng sẽ tương ứng với một cổng giao tiếp, những ứng dụng phổ biến được đặt với số hiệu cổng định trước nhằm định danh duy nhất các ứng dụng đó. Khi máy tính sử dụng dịch vụ nào thì cổng giao tiếp tương ứng với dịch vụ đó sẽ mở.

6. *Giao thức*: Là một tập hợp các quy tắc, quy ước truyền thông chuẩn mà tất cả các thực thể tham gia truyền thông phải tuân theo để có thể kết nối và trao đổi thông tin với nhau.

7. *Thiết bị chuyển mạch*: Là một thiết bị dùng để kết nối các đoạn mạng với nhau.

8. *Tường lửa*: Là rào chắn được lập ra nhằm ngăn chặn người dùng mạng Internet truy cập các thông tin không mong muốn hoặc (và) ngăn chặn người dùng từ bên ngoài truy nhập các thông tin bảo mật nằm trong mạng nội bộ, là một thiết bị phần cứng và (hoặc) phần mềm hoạt động trong môi trường mạng để ngăn chặn một số liên lạc bị cấm bởi chính sách an ninh của cá nhân hay tổ chức.

9. *Bản ghi nhật ký hệ thống thông tin*: Là một tệp tin được tạo ra trên mỗi thiết bị của hệ thống thông tin có chứa tất cả thông tin về các hoạt động xảy ra trên thiết bị đó. Bản ghi nhật ký hệ thống thông tin dùng để phân tích những sự kiện đã xảy ra, nguồn gốc và các kết quả để có các biện pháp xử lý thích hợp.

Chương II
CÔNG TÁC BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN

Điều 3. Xây dựng hệ thống thông tin

Khi xây dựng hệ thống thông tin, các cơ quan, đơn vị cần phải:

1. Tổ chức hệ thống mạng phù hợp để tăng cường tính bảo mật. Các cơ quan, đơn vị có nhiều phòng, ban, đơn vị trực thuộc không nằm trong cùng một khu vực, cần thiết lập mạng riêng ảo để bảo đảm an ninh cho mạng nội bộ. Khi thiết lập các dịch vụ trên môi trường mạng Internet, chỉ cung cấp những chức năng thiết yếu nhất bảo đảm duy trì hoạt động của hệ thống thông tin, hạn chế sử dụng các chức năng, cổng giao tiếp, giao thức và dịch vụ mạng không cần thiết.

2. Đối với việc lắp đặt mạng không dây để kết nối với mạng nội bộ, cần thiết lập, cấu hình các thông số, đặt mật khẩu và thường xuyên thay đổi mật khẩu nhằm bảo đảm công tác bảo mật.

3. Trang bị thiết bị chuyển mạch bảo đảm khả năng cung cấp các chức năng quản trị nhằm tăng cường độ an toàn và bảo mật cho hệ thống mạng.

4. Trang bị, cài đặt tường lửa bảo đảm khả năng xử lý được số lượng kết nối đồng thời cao và chịu được thông lượng cao, hỗ trợ các công nghệ mạng riêng ảo thông dụng và có phần cứng mã hóa tích hợp để tăng tốc độ mã hóa dữ liệu, cung cấp đầy đủ các cơ chế bảo mật, quản lý luồng dữ liệu ra vào và có khả năng bảo vệ hệ thống thông tin trước các loại tấn công từ chối dịch vụ; trang bị thiết bị phát hiện hoặc phòng chống xâm nhập trái phép.

LawSoft * Tel: +84-8-3930 3279 * www.ThuVienPhapLuat.vn

5. Bố trí phòng máy chủ độc lập, bảo đảm khô, thoáng, nguồn điện cung cấp ổn định cao, được trang bị máy điều hòa nhiệt độ và cho vận hành liên tục, được lắp đặt thiết bị chống sét và hệ thống phòng cháy chữa cháy. Phòng máy chủ được giao cho cán bộ có chuyên môn về công nghệ thông tin trực tiếp quản lý, các cán bộ không liên quan không được vào phòng máy chủ.

6. Cài đặt các phần mềm hệ điều hành, phần mềm ứng dụng, phần mềm quản trị cơ sở dữ liệu, phần mềm chống vi-rút máy tính có bản quyền trên các máy chủ, máy trạm, các thiết bị, phương tiện kỹ thuật trong hệ thống mạng; cài đặt các phần mềm tiện ích để đánh giá, tìm kiếm các lỗ hổng bảo mật.

7. Tạo tài khoản và phân quyền người dùng để truy nhập hệ thống thông tin; yêu cầu người dùng đặt mật khẩu với độ an toàn cao; thiết lập giới hạn một số hữu hạn lần đăng nhập sai liên tiếp vào hệ thống thông tin, nếu liên tục đăng nhập sai vượt quá số lần quy định thì hệ thống thông tin phải tự động khóa tài khoản hoặc cô lập tài khoản trong một khoảng thời gian nhất định trước khi tiếp tục cho đăng nhập.

8. Cấu hình hệ thống thông tin bảo đảm ghi nhận đầy đủ các thông tin, sự kiện trong các bản ghi nhật ký hệ thống thông tin; lưu giữ nội dung nhật ký hệ thống thông tin trong khoảng thời gian tối thiểu 1 năm để phục vụ việc quản lý, kiểm soát hệ thống thông tin.

9. Thiết lập phương án dự phòng để bảo đảm hệ thống thông tin hoạt động liên tục 24/24 giờ.

Điều 4. Sử dụng hệ thống thông tin

Khi sử dụng hệ thống thông tin, các cơ quan, đơn vị cần phải:

1. Có kế hoạch kiểm tra, bảo dưỡng định kỳ các thiết bị thuộc hệ thống thông tin; duy trì phù hợp, đúng cách và an toàn các thiết bị với yêu cầu về thời gian và thông số kỹ thuật của nhà cung cấp.

2. Thực hiện quản lý chặt chẽ các tài khoản truy nhập hệ thống thông tin; yêu cầu người dùng thường xuyên thay đổi mật khẩu; định kỳ tổ chức kiểm tra các tài khoản truy nhập hệ thống thông tin; hủy tài khoản truy nhập hệ thống thông tin và thu hồi các tài liệu, hồ sơ, thông tin liên quan tới tài khoản bị hủy bỏ đối với cán bộ, nhân viên đã nghỉ việc hoặc chuyển công tác; tổ chức theo dõi, kiểm soát tất cả các phương pháp truy nhập từ xa tới hệ thống thông tin, bao gồm cả sự truy nhập có chức năng quản trị.

3. Thường xuyên kiểm tra, sao lưu các bản ghi nhật ký hệ thống thông tin để lưu vết những sự kiện đã xảy ra.

4. Thường xuyên cập nhật phiên bản mới, bản vá lỗi của các phần mềm hệ điều hành, phần mềm ứng dụng, phần mềm quản trị cơ sở dữ liệu, phần mềm chống vi-rút máy tính nhằm bảo đảm khả năng phát hiện, ngăn chặn, loại trừ vi-rút máy tính cũng như sự xâm nhập của tin tặc vào hệ thống thông tin; thực hiện chế độ quét vi-rút máy tính thường xuyên.

5. Tổ chức cấp phát tài nguyên trên máy chủ theo danh mục thư mục cho

LawSoft * Tel: +84-8-3930 3279 * www.ThuVienPhapLuat.vn

từng phòng, ban; kiểm tra, giám sát việc chia sẻ tài nguyên, khuyến cáo người sử dụng cân nhắc việc chia sẻ tài nguyên trên các máy trạm, khi sử dụng chức năng chia sẻ tài nguyên cần phải sử dụng mật khẩu để bảo vệ và thực hiện việc thu hồi chức năng này khi đã sử dụng xong.

6. Không phát triển, kiểm thử, cài đặt các ứng dụng thử nghiệm trên hệ thống vận hành chính thức để giảm thiểu rủi ro về an toàn thông tin.

7. 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; cần có các cơ chế đặc biệt nhằm bảo vệ dữ liệu, thông tin nhạy cảm của cơ quan, đơn vị truyền tải qua mạng công cộng để bảo đảm tính toàn vẹn và bí mật của thông tin.

8. Thực hiện định kỳ việc sao lưu dữ liệu hệ điều hành, các phần mềm ứng dụng, phần mềm chuyên ngành, các cơ sở dữ liệu quan trọng phục vụ công tác của cơ quan, đơn vị bằng các phần mềm chuyên dụng, sao chép ra các thiết bị lưu trữ ngoài, thực hiện việc đánh số, dán nhãn để tránh nhầm lẫn và cất giữ ở nơi an toàn; đồng thời thường xuyên kiểm tra để bảo đảm tính sẵn sàng phục hồi và toàn vẹn thông tin.

9. Tắt máy tính trạm hoặc ngưng kết nối mạng trong trường hợp máy tính không sử dụng trong thời gian dài (quá 4 giờ làm việc) để phòng tránh tin tặc lợi dụng chức năng điều khiển từ xa, sử dụng máy tính này tấn công vào các hệ thống thông tin khác; quét vi-rút máy tính trước khi mở các tệp tin kèm theo thư điện tử biết rõ người gửi, các tệp tin tải về từ Internet, các tệp tin trong các thiết bị lưu trữ ngoài và không được mở các tệp tin kèm theo thư điện tử có nguồn gốc không rõ ràng để phòng ngừa vi-rút máy tính xâm nhập vào máy tính; đặt mật khẩu truy nhập vào máy tính, đồng thời thiết lập chế độ bảo vệ màn hình có sử dụng mật khẩu bảo vệ sau một khoảng thời gian nhất định không sử dụng máy tính.

10. Thường xuyên theo dõi hoạt động của hệ thống thông tin. Khi phát hiện sự cố như máy chủ bị tấn công, cần thông báo ngay cho Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ khắc phục sự cố.

Điều 5. Nâng cấp hệ thống thông tin

Khi nâng cấp hệ thống thông tin, các cơ quan, đơn vị cần phải:

1. Rà soát, đánh giá hệ thống hiện có để lựa chọn phương án tối ưu trên cơ sở sử dụng hạ tầng, các cơ sở dữ liệu, các giải pháp bảo mật,... hiện có.

2. Sau khi nâng cấp hệ thống, cần bổ sung các biện pháp kỹ thuật để đảm bảo hệ thống hoạt động tốt.

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

Điều 6. Trách nhiệm của các cơ quan, đơn vị

1. Xây dựng quy chế nội bộ bảo đảm an toàn, an ninh thông tin của cơ quan, đơn vị trên cơ sở nội dung quy định tại Điều 3, Điều 4 và Điều 5 Quy chế này, trong đó quy định rõ quyền và trách nhiệm của từng bộ phận, cán bộ, công

LawSoft * Tel: +84-8-3930 3279 * www.ThuVienPhapLuat.vn

chức, viên chức.

2. Lập dự toán kinh phí chi thường xuyên hàng năm cho các hoạt động liên quan đến việc bảo đảm an toàn, an ninh thông tin của cơ quan, đơn vị.

3. Phối hợp với Sở Thông tin và Truyền thông, Công an tỉnh để phổ biến các kiến thức cơ bản về máy tính, mạng máy tính, an toàn, an ninh thông tin cho cán bộ, công chức, viên chức trước khi truy nhập và sử dụng hệ thống thông tin; bố trí cán bộ có chuyên môn hoặc có am hiểu và được đào tạo sâu về công nghệ thông tin bảo đảm an toàn, an ninh thông tin trước khi tiến hành các hoạt động quản lý, vận hành, bảo trì, nâng cấp hệ thống thông tin; tạo điều kiện cho cán bộ, công chức, viên chức được học tập, tiếp thu công nghệ, kiến thức về an toàn, an ninh thông tin, đặc biệt là cán bộ phụ trách về công nghệ thông tin.

4. Phối hợp chặt chẽ với Công an trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an ninh thông tin. Tạo điều kiện thuận lợi và phối hợp với các cơ quan chức năng trong công tác kiểm tra về an toàn, an ninh thông tin, điều tra nguyên nhân gây ra sự cố và khắc phục sự cố.

5. Báo cáo định kỳ hàng năm về tình hình an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan, đơn vị gửi về Sở Thông tin và Truyền thông trước ngày 25 tháng 12 để tổng hợp chung báo cáo Ủy ban nhân dân tỉnh.

Điều 7. Trách nhiệm của Sở Thông tin và Truyền thông

1. Tham mưu Ủy ban nhân dân tỉnh về công tác bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan, đơn vị trên địa bàn tỉnh, cụ thể: về quy trình, chính sách chung; thẩm định đầu tư thiết bị phần cứng, phần mềm, hạ tầng mạng truyền thông; đào tạo về an toàn thông tin cho cán bộ, công chức, viên chức; tổ chức các hội thảo chuyên ngành về ứng cứu sự cố máy tính, đảm bảo an toàn hệ thông thông tin; tổ chức bảo đảm an toàn thông tin cho các hệ thống thông tin dùng chung cấp tỉnh phục vụ sự lãnh đạo, điều hành của lãnh đạo tỉnh được nhanh chóng, an toàn, hiệu quả.

2. Chủ trì, phối hợp với Công an tỉnh, Báo Hải Dương, Đài Phát thanh và Truyền hình tỉnh và các cơ quan báo chí khác đẩy mạnh tuyên truyền nâng cao nhận thức về an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh.

3. Thông báo cho các cơ quan, đơn vị biết và hướng dẫn các biện pháp kỹ thuật nghiệp vụ phòng ngừa, ngăn chặn các nguy cơ gây mất an toàn thông tin.

4. Chủ trì, phối hợp với các cơ quan, đơn vị liên quan xử lý, ứng cứu các sự cố máy tính trong các cơ quan, đơn vị.

5. Lập dự toán kinh phí chi thường xuyên bảo đảm cho các hoạt động ứng cứu sự cố máy tính của hệ thống thông tin chung toàn tỉnh (như Trung tâm tích hợp dữ liệu, hệ thống giao ban trực tuyến, Cổng thông tin điện tử, hệ thống thư điện tử, hạ tầng truyền dẫn,...).

6. Chủ trì, phối hợp với Công an tỉnh và các ngành liên quan tổ chức kiểm tra

LawSoft * Tel: +84-8-3930 3279 * www.ThuVienPhapLuat.vn

theo định kỳ hoặc đột xuất khi phát hiện có dấu hiệu, hành vi vi phạm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin và xử phạt theo quy định.

Điều 8. Trách nhiệm của Công an tỉnh

1. Tham mưu Ủy ban nhân dân tỉnh về công tác bảo đảm an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan, đơn vị trên địa bàn tỉnh; đào tạo, bồi dưỡng kiến thức về an ninh thông tin cho cán bộ, công chức, viên chức.

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

3. Phối hợp với Sở Thông tin và Truyền thông và các ngành liên quan tiến hành kiểm tra theo định kỳ hoặc đột xuất khi phát hiện có dấu hiệu, hành vi vi phạm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin.

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

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 9. Điều khoản thi hành

Sở Thông tin và Truyền thông chủ trì, phối hợp với các cơ quan, đơn vị triển khai thực hiện nghiêm Quy chế này.

Trong quá trình thực hiện, nếu có vướng mắc, phát sinh, các cơ quan, đơn vị 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. UỶ BAN NHÂN DÂN TỈNH
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Nguyễn Dương Thái

LawSoft * Tel: +84-8-3930 3279 * www.ThuVienPhapLuat.vn