UBND TỈNH HÀ TĨNH
SỞ KHOA HỌC VÀ CÔNG NGHỆ

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

Số: 1354 / QĐ-SKHCN

Hà Tĩnh, ngày 26 tháng 12 năm 2013

QUYẾT ĐỊNH
Ban hành Quy chế đảm bảo an toàn thông tin trong quản lý, vận hành và khai thác hệ thống thông tin tại Sở Khoa học và Công nghệ Hà Tĩnh

GIÁM ĐỐC SỞ KHOA HỌC VÀ CÔNG NGHỆ

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

Căn cứ 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; 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 897/CT-TTg ngày 10/6/2011 của Thủ tướng Chính phủ về tăng cường triển khai các hoạt động đảm bảo an toàn thông tin số;

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 07/2011/QĐ-UBND ngày 25/5/2011 của UBND tỉnh Hà Tĩnh về việc ban hành Quy định về tổ chức thực hiện ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước trên địa bàn tỉnh;

Căn cứ Quyết định số 27/2008/QĐ-UBND ngày 01/9/2008 về chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức Sở Khoa học và Công nghệ;

Theo đề nghị của Chánh Văn phòng, Trưởng phòng Thông tin – Tư liệu,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn thông tin trong quản lý, vận hành và khai thác hệ thống thông tin tại Sở Khoa học và Công nghệ Hà Tĩnh.

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

Chánh Văn phòng, phòng Thông tin – Tư liệu; các đơn vị và cá nhân có liên quan căn cứ Quyết định thi hành./.

Nơi nhận:
- Như Điều 2;
- Ban Giám đốc;
- Các đơn vị cấp 2;
- Lưu VT.

GIÁM ĐỐC

Đỗ Khoa Văn

UBND TỈNH HÀ TĨNH
SỞ KHOA HỌC VÀ CÔNG NGHỆ

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

Hà Tĩnh, ngày 26 tháng 12 năm 2013

QUY CHẾ
Đảm bảo an toàn thông tin trong quản lý, vận hành và khai thác hệ thống thông tin tại Sở Khoa học và Công nghệ Hà Tĩnh

(Ban hành kèm theo Quyết định số: 1354/QĐ-SKHCN ngày 26 tháng 12 năm 2013 của Sở Khoa học và Công nghệ Hà Tĩnh)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi, đối tượng áp dụng

Quy chế này quy định về công tác bảo an toàn thông tin trong quản lý, vận hành và khai thác hệ thống thông tin tại Sở Khoa học và Công nghệ Hà Tĩnh; công chức, viên chức tham gia quản lý; công chức, viên chức và các đối tượng tham gia vận hành và khai thác hệ thống 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 hệ thống thông tin tránh bị truy cập, sử dụng, tiết lộ, gián đoạn, sửa đổi, gián đoạn, sửa đổi, xâm hại hoặc phá hoại trái phép nhằm đảm bảo tính nguyên vẹn, tính bảo mật, tính sẵn sàng và tính khả dụng của thông tin.

2. Hệ thống thông tin là tập hợp các thiết bị viễn thông, công nghệ thông tin ban gồm phần cứng, phần mềm 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.

Chương II
CÔNG TÁC BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 3. Các biện pháp quản lý nhằm đảm bảo an toàn thông tin.

1. Phòng Thông tin - Tư liệu thường xuyên phổ biến, hướng dẫn, cập nhật và quán triệt đầy đủ kiến thức cơ bản về an toàn thông tin và công tác đảm bảo an toàn thông tin đến từng cán bộ, công chức, viên chức và người lao động.

2. Cán bộ chuyên trách về CNTT đảm nhận Chuyên trách về công tác an toàn thông tin trong Sở; tham mưu giúp Lãnh đạo Sở ban hành cơ chế chính sách đảm bảo an toàn thông tin, đảm bảo bí mật nhà nước và triển khai các biện pháp nhằm đảm bảo an toàn thông tin trong Sở; thường xuyên giám sát tất cả các truy cập, kiểm tra, đánh giá, báo cáo tình hình, các nguy cơ, mức độ mất an

toàn thông tin có thể xảy ra và các biện pháp phòng ngừa, ngăn chặn, khắc phục kịp thời nhằm đảm bảo mức độ an toàn cao nhất cho hệ thống thông tin của Sở.

3. Đối với cán bộ, công chức, viên chức đã nghỉ hoặc chuyển công tác, cán bộ chuyên trách phải thu hồi, vô hiệu hóa quyền truy cập hoặc loại bỏ tài khoản khỏi hệ thống ngay sau khi bàn giao công việc, song vẫn đảm bảo khả năng truy cập vào các hồ sơ công việc có liên quan đến tài khoản của người đó.

4. Giám đốc công nghệ thông tin - CIO của Sở có trách nhiệm chỉ đạo làm tốt công tác an toàn thông tin tại Sở; có kế hoạch về công tác đảm bảo an toàn thông tin hàng năm và bố trí đủ nguồn lực để thực hiện.

Điều 4. Các biện pháp kỹ thuật đảm bảo an toàn thông tin

1. Quản lý đăng nhập hệ thống: Các hệ thống thông tin cần giới hạn số lần đăng nhập vào hệ thống. Hệ thống tự động khóa tài khoản hoặc cô lập tài khoản khi liên tục đăng nhập sai vượt quá số lần quy định. Yêu cầu người sử dụng đặt mật khẩu với độ an toàn cao, giám sát, nhắc nhở khuyến cáo nên thay đổi thường xuyên mật khẩu.

2. Quản lý hệ thống mạng không dây: Thiết lập mật khẩu nhằm tăng cường công tác bảo mật.

3. Quản lý Logfile: Hệ thống thông tin cần ghi nhận các sự kiện: quá trình đăng nhập vào hệ thống, các thao tác cấu hình hệ thống. Thường xuyên kiểm tra, sao lưu (backup) các logfile theo từng tháng để lưu vết theo dõi, xác định những sự kiện đã xảy ra của hệ thống và hạn chế việc tràn logfile gây ảnh hưởng đến hoạt động của hệ thống.

4. Chống mã độc, virus: Lựa chọn, triển khai các phần mềm chống virus trên các máy chủ, hỗ trợ người sử dụng cài đặt các phần mềm này trên máy trạm. Thường xuyên cập nhật các phiên bản (Version) mới, các bản vá lỗi của các phần mềm chống virus để bảo đảm chương trình quét virus của cơ quan trên các máy chủ, máy trạm luôn được cập nhật mới nhất, thiết lập chế độ quét thường xuyên ít nhất là hàng tuần.

Điều 5. Các nghiệp vụ đảm bảo an toàn thông tin

1. Đối với các phòng, đơn vị:

a) Công tác đảm bảo an toàn thông tin tuân thủ theo tiêu chuẩn, quy chuẩn kỹ an toàn thông tin và yêu cầu bắt buộc đối với các dự án đầu tư từ khâu thiết kế, thi công, vận hành đến việc nâng cấp, thay thế, hủy bỏ các hệ thống thông tin.

b. Không sử dụng máy tính có kết nối Internet để đánh máy, in, lưu trữ tài liệu mật. Mọi thông tin thuộc bí mật nhà nước khi lưu trữ và truyền đi trên môi trường mạng phải được mã hóa và quản lý theo quy định của pháp luật về cơ yếu.

c) Khi mua sắm, tiếp nhận thiết bị CNTT mới phải tiến hành kiểm tra nhằm phát hiện các "chíp điện tử" được gắn trái phép trong thiết bị.

d) Việc thanh lý, tiêu hủy thiết bị, phần mềm, vật mang thông tin phải đảm bảo yêu cầu không để lộ, lọt thông tin nhà nước; phải có quy trình cụ thể và lưu giữ hồ sơ, biên bản thanh lý, tiêu hủy.

2. Đối với cán bộ chuyên trách về an toàn thông tin:

a) Thực hiện Điều 3, Điều 4 của Quy chế này.

b) Kiểm tra, cấu hình và thường xuyên cập nhật cấu hình chuẩn cho các thành phần của hệ thống thông tin; thiết lập cấu hình một cách chặt chẽ nhất đảm bảo mức an toàn thông tin cao nhất cho hệ thống, song vẫn đảm bảo tính sẵn sàng và hoạt động liên tục.

c) Thiết lập, quản lý và thường xuyên thay đổi mật khẩu cho các thành phần hệ thống thông tin trong cơ quan song không làm xáo trộn hoạt động thường xuyên của người dùng; yêu cầu mọi người phải thường xuyên thay đổi mật khẩu truy cập của mình.

d) Tổ chức quản lý định danh đối với tất cả người dùng tham gia khai thác hệ thống thông tin; thường xuyên sao lưu dữ liệu trong hệ thống thông tin của Sở; đảm bảo tính sẵn sàng và toàn vẹn dữ liệu.

đ) Thường xuyên kiểm tra, sao lưu nhật ký của hệ thống thông tin, để lưu vết, theo dõi và xác định những sự kiện đã xảy ra trong hệ thống.

e) Áp dụng biện pháp quản lý và kỹ thuật phù hợp với tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin để phòng, chống nguy cơ, khắc phục sự cố an toàn thông tin.

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

a) Thường xuyên cập nhật những chính sách, các tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin, tuân thủ hướng dẫn về an toàn thông tin thuộc phạm vi cá nhân quản lý, đồng thời có trách nhiệm bảo vệ an toàn thông tin chung theo quy định.

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 thực hiện việc thu hồi chia sẻ khi đã sử dụng xong.

c) Đặt mật khẩu truy cập vào máy tính được cấp cho mình sử dụng, đồng thời thiết lập chế độ bảo vệ màn hình có sử dụng mật khẩu bảo vệ; sử dụng các thiết bị lưu trữ an toàn, đúng cách để phòng ngừa virus, các phần mềm gián điệp xâm nhập vào máy tính.

d) Bảo vệ, quản lý tài khoản được giao để đăng nhập vào các hệ thống thông tin, thường xuyên thay đổi mật khẩu, đảm bảo mật khẩu đủ mạnh gồm các ký tự số, chữ và các ký tự đặc biệt; thường xuyên lưu trữ, sao lưu dữ liệu của cá nhân đảm bảo các yêu cầu về an toàn thông tin.

đ) Chỉ sử dụng hệ thống thư điện tử, hệ thống quản lý văn bản và điều hành tác nghiệp, các hệ thống thông tin khác của cơ nhà nước để gửi, nhận, đăng tải văn bản điện tử trong hoạt động.

e) Phải thực hiện quét virus trước khi mở các tập tin đính kèm theo thư điện tử, không mở các thư chưa rõ người gửi hoặc tập tin đính kèm có nguồn gốc không rõ ràng để tránh virus, phần mềm gián điệp xâm nhập vào máy tính, cảnh giác cao độ với thư rác, thư không rõ nguồn gốc.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 6. Trách nhiệm của Giám đốc CNTT-CIO

1. Giám đốc CNTT-CIO của Sở chịu trách nhiệm toàn diện trước Ủy ban nhân dân tỉnh trong công tác đảm bảo an toàn thông tin của Sở, đồng thời thực hiện nghiêm túc các quy chế này.

2. Khi có sự cố hoặc nguy cơ mất an toàn thông tin, kịp thời áp dụng mọi biện pháp tại chỗ, phối hợp chặt chẽ với các tổ chức, đơn vị liên quan để ngăn chặn, khắc phục, hạn chế thiệt hại và báo cáo bằng văn bản cho cơ quan cấp trên quản lý trực tiếp và 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 cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông để được hướng dẫn và hỗ trợ kịp thời.

3. Phối hợp chặt chẽ với Sở Thông tin và Truyền thông, Công an tỉnh trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm trái phép gây mất an toàn thông tin; phối hợp và tạo điều kiện thuận lợi cho các cơ quan chức năng tham gia khắc phục sự cố, tuân thủ các hướng dẫn của các cơ quan chức năng.

4. Phối hợp với Đoàn kiểm tra để triển khai công tác kiểm tra, khắc phục sự cố được nhanh chóng và đạt hiệu quả; đồng thời cung cấp đầy đủ các thông tin khi Đoàn kiểm tra yêu cầu xuất trình.

Điều 7. Trách nhiệm của cán bộ, công chức, viên chức

1. Trách nhiệm của cán bộ chuyên trách:

a) Chịu trách nhiệm triển khai các biện pháp quản lý, nghiệp vụ, kỹ thuật nhằm đảm bảo an toàn thông tin tại đơn vị mình theo các quy định của Quy chế này.

b) Phối hợp với các cá nhân, đơn vị liên quan trong việc kiểm tra, phát hiện và khắc phục sự cố mất an toàn thông tin.

c) Tham mưu chuyên môn và vận hành an toàn hệ thống thông tin của Sở theo nhiệm vụ của cán bộ chuyên trách.

2. Trách nhiệm của cán bộ, công chức, viên chức trong Sở:

a) Nghiêm chỉnh tuân thủ các quy định của Quy chế này và các quy định nội bộ cũng như các quy định khác của pháp luật, nâng cao ý thức cảnh giác, trách nhiệm bảo đảm an toàn thông tin của Sở; không được xâm phạm an toàn thông tin của tổ chức, cá nhân khác.

b) Thường xuyên cập nhật các chính sách, tiêu chuẩn, quy chuẩn, hướng dẫn đảm bảo an toàn thông tin của Sở, của tỉnh, của các bộ ngành Trung ương.

c) Bảo đảm an toàn thông tin đối với các thành phần của hệ thống thông tin thuộc thẩm quyền quản lý. Khi phát hiện thư điện tử giả mảo, các hành vi xâm hại an toàn thông tin hoặc sự cố mất an toàn thông tin phải báo cáo ngay với cấp trên và cán bộ chuyên trách để kịp thời xử lý.

d) Tham gia đầy đủ các chương trình phổ biến, bồi dưỡng về an toàn thông tin do cơ quan tổ chức.

Chương V
KHEN THƯỞNG, XỬ LÝ VI PHẠM

Điều 8. Khen thưởng

Các phòng, ban, đơn vị trực thuộc; cán bộ, công chức, viên chức và người lao động thực hiện tốt Quy chế này đem lại hiệu quả thiết thực sẽ được xem xét đánh giá khen thưởng.

Điều 9. Xử lý vi phạm

Các phòng, ban, đơn vị trực thuộc; cán bộ, công chức, viên chức và người lao động có hành vi vi phạm quy chế này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật theo trách nhiệm, xử phạt hành chính hoặc bị truy cứu trách nhiệm hình sự. Nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật hiện hành.

Trong quá trình thực hiện nếu có phát sinh khó khăn, vướng mắc cần sửa đổi, bổ sung các phòng ban, đơn vị kịp thời báo cáo về phòng Thông tin – Tư liệu tổng hợp trình Lãnh đạo sở xem xét, giải quyết./.

GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ KHOA HỌC VÀ CÔNG NGHỆ
TỈNH THÁI NGUYÊN

Đỗ Khoa Văn