UBND TỈNH KON TUM
SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG
Số: 250/QĐ-STNMT

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

Kon Tum, ngày 27 tháng 10 năm 2016

QUYẾT ĐỊNH

Ban hành Quy chế đảm bảo an toàn thông tin trong quản lý, vận hành và khai thác hệ thống thông tin trên môi trường mạng tại Sở Tài nguyên và Môi trường tỉnh Kon Tum

GIÁM ĐỐC SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG KON TUM

Căn cứ Chỉ thị số 897/CT-TTg ngày 10/6/2011 của Thủ tướng Chính phủ về việc 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 đảm bảo an toàn thông tin trên Mạng truyền số liệu chuyên dùng của các cơ quan Đảng và Nhà nước;

Căn cứ Quyết định số 05/2016/QĐ-UBND ngày 05/02/2016 của Ủy ban nhân dân tỉnh Kon Tum về việc ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Tài nguyên và Môi trường tỉnh Kon Tum;

Căn cứ Quyết định số 24/2016/QĐ-UBND ngày 17/06/2016 Ủy ban nhân dân tỉnh Kon Tum Về việc 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 tỉnh Kon Tum;

Căn cứ Kế hoạch số 2300/KH-UBND ngày 22/09/2016 của của Ủy ban nhân dân tỉnh Kon Tum về ứng dụng CNTT trong hoạt động của các cơ quan nhà nước tỉnh Kon Tum giai đoạn 2016-2020;

Xét đề nghị của Chánh Văn phòng Sở và Giám đốc Trung tâm Công nghệ thông tin Tài nguyên và Môi trường,

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 trên môi trường mạng tại Sở Tài nguyên và Môi trường tỉnh Kon Tum.

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

Điều 3. Chánh Văn phòng Sở; Giám đốc Trung tâm Công nghệ thông tin Tài nguyên và Môi trường; Trưởng các phòng, đơn vị và công chức, viên chức, người lao động trực thuộc Sở chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Sở Thông tin và Truyền thông (b/c);
- GĐ và các PGĐ Sở;
- Các phòng, đơn vị thuộc Sở;
- Lưu: VT, VP, TTCNTT.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG
TỈNH KON TUM

Phạm Đức Hạnh

UBND TỈNH KON TUM
SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG

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

QUY CHẾ
Đảm bảo an toàn thông tin trong quản lý, vận hành và khai thác các hệ thống thông tin trên môi trường mạng tại Sở Tài nguyên và Môi trường tỉnh Kon Tum

(Ban hành kèm theo Quyết định số 250 /QĐ-STNMT ngày 21 tháng 10 năm 2016 của Sở Tài nguyên và Môi trường tỉnh Kon Tum)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi, đối tượng áp dụng

Quy chế này quy định về công tác đảm bảo an toàn thông tin trong quản lý, vận hành và khai thác các hệ thống thông tin tại Sở Tài nguyên và Môi trường, bao gồm các phòng, đơn vị trực thuộc; công chức, viên chức, người lao động thuộc Sở và các đối tượng tham gia vận hành, khai thác các 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, xâm hại hoặc phá hoại trái phép nhằm bảo đảm 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 bao 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.

3. Mạng truyền số liệu chuyên dùng của Ủy ban nhân dân tỉnh, mạng truyền dẫn tốc độ cao, sử dụng phương thức chuyển mạch nhãn đa giao thức trên nền giao thức liên mạng (IP/MPLS) sử dụng riêng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan Đảng, Nhà nước do cơ quan viễn thông xây dựng, quản lý, vận hành lắp đặt tại Sở Tài nguyên và Môi trường (sau đây gọi là Mạng chuyên dùng).

4. Cán bộ chuyên trách công nghệ thông tin được hiểu là cán bộ được giao nhiệm vụ hoặc giao kiêm nhiệm để giúp lãnh đạo về công tác công nghệ thông tin của Sở hoặc đơn vị thuộc Sở.

5. Tổ chuyên trách ứng dụng công nghệ thông tin của Sở gồm các thành viên sau: Chánh văn phòng-Tổ trưởng; Giám đốc Trung tâm Công nghệ thông tin Tài nguyên và Môi trường-Tổ phó; đại diện các phòng, đơn vị thuộc Sở; cán bộ chuyên trách công nghệ thông tin của Sở và cán bộ chuyên trách công nghệ thông tin của Trung tâm Công nghệ thông tin Tài nguyên và Môi trường.

Chương II
CÔNG TÁC ĐẢM BẢO AN TOÀN THÔNG TIN

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

1. Trưởng các phòng, đơn vị thuộc Sở có trách nhiệm thường xuyên phổ biến, hướng dẫn, cập nhật, quán triệt đầy đủ các quy định pháp luật, các văn bản chỉ đạo, hướng dẫn về an toàn thông tin, công tác đảm bảo an toàn thông tin đến từng công chức, viên chức, người lao động thuộc phòng, đơn vị mình; các đối tượng cần thiết khi cấp quyền truy cập và sử dụng hệ thống thông tin.

2. Cán bộ chuyên trách về công nghệ thông tin của mỗi đơn vị thuộc Sở đảm nhận chuyên trách về công tác an toàn thông tin trong cơ quan; tham mưu giúp lãnh đạo cơ quan ban hành kế hoạch, quy chế nội bộ 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 đơn vị; thường xuyên giám sát tất cả các truy cập (bao gồm cả truy cập đặc quyền); 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 cơ quan.

3. Cán bộ chuyên trách về công nghệ thông tin của mỗi đơn vị thuộc Sở phải quản lý chặt chẽ mọi tài khoản trong hệ thống thông tin, bắt đầu từ khâu tạo mới, kích hoạt, cấp phát, thu hồi, sửa đổi tài khoản, đổi mật khẩu, vô hiệu hóa, loại bỏ các tài khoản cho đến việc cấp và sửa đổi quyền truy cập, đồng thời đảm bảo kiểm tra tình trạng hoạt động của mỗi tài khoản ít nhất một lần trong năm.

4. Đối với công chức, viên chức, người lao động đã nghỉ việc hoặc chuyển đơn vị công tác, phải thu hồi, vô hiệu hóa quyền truy cập hoặc loại bỏ tài khoản khỏi hệ thống thông tin ngay sau khi bàn giao công việc, song vẫn đảm bảo khả năng truy cập vào các hồ sơ công việc có liên quan tới tài khoản của người đó.

5. Các tổ chức và cá nhân không phải là phòng, đơn vị và công chức, viên chức, người lao động thuộc Sở khi tham gia khai thác hệ thống thông tin của Sở đều phải tuân thủ các quy định về đảm bảo an toàn thông tin tại quy chế này.

6. Tổ chuyên trách ứng dụng công nghệ thông tin của Sở đảm nhận trách nhiệm quản lý về an toàn thông tin tại Sở; trình phê duyệt kế hoạch về công tác đảm bảo an toàn thông tin hàng năm và nguồn lực để thực hiện kế hoạch đó; phối hợp với các phòng, đơn vị thuộc Sở và các cơ quan liên quan để thực hiện các nhiệm vụ về đảm bảo an toàn thông tin theo quy định của pháp luật.

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

1. Hệ thống thông tin tại Sở Tài nguyên và Môi trường được áp dụng các biện pháp đăng nhập trước khi truy cập, có cơ chế giới hạn số lần đăng nhập sai liên tiếp.

2. Hệ thống thông tin tại Sở có tính năng tự động ghi nhận được lịch sử quá trình đăng nhập hệ thống, các thao tác cấu hình hệ thống, quá trình truy xuất hệ thống vào các thông tin liên quan đến an toàn thông tin.

3. Hệ thống thông tin tại Sở phải có cơ chế sao lưu, phục hồi dữ liệu ở mức người dùng và mức hệ thống; dữ liệu sao lưu phải được quản lý chặt chẽ, an toàn, được kiểm tra thường xuyên để đảm bảo tính sẵn sàng và toàn vẹn dữ liệu.

4. Hạ tầng kỹ thuật của hệ thống thông tin tại Sở phải được trang bị đủ, đạt yêu cầu kỹ thuật, đảm bảo vận hành liên tục, có khả năng kiểm soát, phát hiện và ngăn chặn các truy cập trái phép, các loại tấn công từ bên ngoài; cài đặt các phần mềm phòng chống virus, thư rác, chống mã độc cho thiết bị đầu cuối như máy trạm, máy chủ.

5. Phải tuân thủ đầy đủ các quy định, các yêu cầu kỹ thuật an toàn về điện, chống sét; có biện pháp bảo vệ, dự phòng; có kế hoạch phòng chống các nguy cơ do mất cắp, cháy nổ, lũ lụt,…và khôi phục hệ thống nếu có sự cố xảy ra.

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

1. Đối với các phòng, đơn vị trực thuộc:

a) Công tác đảm bảo an toàn thông tin phải tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin và là 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, huỷ bỏ các hệ thống thông tin.

b) Không sử dụng máy tính có kết nối mạng 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, khuyến khích ứng dụng, sử dụng chữ ký số trong giao dịch điện tử.

c) Khi mua sắm, tiếp nhận thiết bị công nghệ thông tin 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 các thiết bị, phần mềm, vật mang thông tin của các phòng, đơn vị thuộc Sở phải đảm bảo yêu cầu không để lộ, lọt thông tin nhà nước; phải có quy trình cụ thể và phải lưu giữ hồ sơ, biên bản thanh lý, tiêu hủy.

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

a) Tham mưu triển khai, thực hiện các nội dung của Điều 3, Điều 4 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 của hệ thống thông tin trong cơ quan nhưng không làm xáo trộn hoạt động thường xuyên của người dùng; nhắc nhở người dùng phải định kỳ thay đổi mật khẩu truy cập của mình.

d) Quản lý định danh đối với tất cả người dùng tham gia khai thác hệ thống thông tin; định kỳ sao lưu dữ liệu trong hệ thống thông tin của cơ quan; 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 và khắc phục sự cố an toàn thông tin.

3. Đối với công chức, viên chức và người lao động thuộc Sở:

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 dữ liệu (sharing), khi sử dụng chức năng này cần bật thuộc tính bảo mật bằng mật khẩu và thực hiện việc thu hồi chức năng sharing 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 (screen saver) có sử dụng mật khẩu bảo vệ sau một khoảng thời gian nhất định không sử dụng máy tính; 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, định kỳ ít nhất 1 tháng thay đổi mật khẩu một lần, 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 trực tuyến, cổng/trang thông tin điện tử, các hệ thống thông tin khác của cơ quan Nhà nước để gửi, nhận, đăng tải văn bản điện tử trong hoạt động của Sở Tài nguyên và Môi trường Kon Tum.

e) 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 xâm nhập vào máy tính, cảnh giác cao độ đối với thư rác, thư không rõ nguồn gốc.

Điều 6. Đảm bảo an toàn thông tin trên mạng truyền số liệu chuyên dùng

1. Các phòng, đơn vị thuộc Sở có sử dụng Mạng chuyên dùng, áp dụng các biện pháp kỹ thuật cần thiết để bảo đảm an toàn thông tin trên mạng chuyên dùng, bao gồm:

a) Có các biện pháp bảo vệ nhằm ngăn chặn việc truy cập trái phép vào mạng chuyên dùng.

b) Không tự thay đổi kết nối, thông số thiết lập mạng của các thiết bị liên quan đến mạng chuyên dùng không thuộc thẩm quyền, gây xung đột tài nguyên, ảnh hưởng đến việc vận hành hệ thống mạng chuyên dùng.

c) Tuân thủ đầy đủ các quy định về an toàn thông tin, các yêu cầu kỹ thuật an toàn về sử dụng điện; phòng chống sét, phòng chống hỏa hoạn, thiên tai.

d) Phối hợp chặt chẽ với điểm đăng ký dịch vụ (cơ quan viễn thông), với Sở Thông tin và Truyền thông để áp dụng các biện pháp cần thiết bảo đảm an toàn thông tin trên mạng chuyên dùng và khắc phục sự cố liên quan đến hoạt động điều hành của cơ quan.

đ) Phân tích kết nối Internet (không qua Mạng chuyên dùng) của cơ quan với mạng chuyên dùng để bảo đảm không làm gia tăng nguy cơ mất an toàn thông tin đối với mạng chuyên dùng.

2. Phải thường xuyên tiến hành kiểm tra, đánh giá về mức độ an toàn thông tin trên mạng chuyên dùng tại đơn vị mình. Quy trình kiểm tra, đánh giá phải đáp ứng các yêu cầu sau đây:

a) Tuân thủ theo quy định của pháp luật về an toàn thông tin.

b) Kiểm tra và đánh giá hoạt động của hệ thống tường lửa, bộ tập trung người dùng mạng riêng ảo (nếu có), dải địa chỉ IP và hệ thống tên miền của cơ quan.

c) Kiểm định hạ tầng kỹ thuật được thiết lập tại cơ quan có kết nối với mạng chuyên dùng phù hợp với tiêu chuẩn, quy chuẩn về công nghệ thông tin và truyền thông và cấu hình mạng chuyên dùng.

3. Các phòng, đơn vị chủ động xác định những vấn đề phát sinh, tham mưu đề xuất những giải pháp nâng cấp mở rộng phần mạng chuyên dùng thuộc đơn vị mình bằng văn bản tới Tổ chuyên trách ứng dụng công nghệ thông tin của Sở, các cơ quan chức năng nhằm bảo đảm việc sử dụng và khai thác mạng chuyên dùng có hiệu quả nhất.

4. Các phòng, đơn vị ưu tiên sử dụng cán bộ chuyên trách của mình (nếu có) để bảo đảm an toàn mạng và bảo mật thông tin trên mạng chuyên dùng. Trường hợp có sự cố nghiêm trọng vượt quá khả năng khắc phục của phòng, đơn

vị phải phối hợp với Tổ chuyên trách ứng dụng công nghệ thông tin của Sở và cơ quan có chức năng để thực hiện khắc phục sự cố kịp thời, nhanh chóng.

5. Hàng năm các phòng, đơn vị đề nghị xem xét, bố trí kinh phí phù hợp cho hoạt động bảo đảm an toàn thông tin trên mạng chuyên dùng.

6. Các phòng, đơn vị có trách nhiệm quản lý và bảo quản thiết bị của mạng chuyên dùng đã được giao, tránh làm mất, làm hỏng, thất lạc thiết bị; ban hành quy chế nội bộ về an toàn thông tin trên mạng chuyên dùng.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 7. Trách nhiệm của các đơn vị trực thuộc Sở.

1. Thủ trưởng các đơn vị thuộc Sở chịu trách nhiệm trước Giám đốc Sở 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, kịp thời áp dụng mọi biện pháp tại chỗ, phối hợp với các tổ chức, đơn vị liên quan để ngăn chặn, khắc phục, hạn chế thiệt hại và báo cáo bằng văn bản về Tổ chuyên trách ứng dụng công nghệ thông tin của Sở để xử lý và báo cáo lãnh đạo Sở. Trường hợp có sự cố nghiêm trọng vượt quá khả năng khắc phục phải báo cáo lãnh đạo Sở và phối hợp với Sở Thông tin và Truyền thông để được hướng dẫn và hỗ trợ kịp thời.

3. Phối hợp chặt chẽ với Tổ chuyên trách ứng dụng công nghệ thông tin của Sở, 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. Các đơn vị thuộc Sở phải phối hợp với đoàn kiểm tra của các cơ quan chức năng để triển khai công tác kiểm tra, cung cấp đầy đủ các thông tin khi đoàn kiểm tra về an toàn thông tin yêu cầu.

Điều 8. Trách nhiệm của Tổ chuyên trách ứng dụng công nghệ thông tin của Sở

1. Tham mưu giúp Giám đốc Sở trong công tác quản lý về công tác đảm bảo an toàn thông tin trong cơ quan Sở Tài nguyên và Môi trường.

2. Chủ trì tham mưu lãnh đạo Sở phối hợp tổ chức kiểm tra định kỳ hoặc đột xuất khi phát hiện có dấu hiệu, hành vi vi phạm an toàn thông tin, xử lý nghiêm các hành vi vi phạm an toàn thông tin theo quy định của pháp luật.

3. Hướng dẫn các tiêu chí và quy trình kỹ thuật nhằm đảm bảo an toàn thông tin; kiểm tra công tác đảm bảo an toàn thông tin; tham mưu cử công chức tham gia các chương trình đào tạo, bồi dưỡng và tuyên truyền về an toàn thông tin.

4. Hướng dẫn các phòng, đơn vị thực hiện các báo cáo về sự cố mất an toàn thông tin và kết quả thực hiện công tác đảm bảo an toàn thông tin.

5. Tùy theo mức độ sự cố, phối hợp các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố mất an toàn thông tin.

6. Đưa nội dung đảm bảo an toàn thông tin vào kế hoạch ứng dụng công nghệ thông tin hàng năm của Sở; dự toán kinh phí để triển khai công tác đảm bảo an toàn thông tin cho các hệ thống thông tin của Sở.

Điều 9. Trách nhiệm của các cá nhân

1. Trách nhiệm của cán bộ chuyên trách về công tác an toàn thông tin tại các đơn vị:

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 và quy định về an toàn thông tin của đơn vị mình.

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) Chịu trách nhiệm tham mưu chuyên môn và vận hành an toàn hệ thống thông tin của đơn vị theo nhiệm vụ của cán bộ chuyên trách.

2. Trách nhiệm của công chức, viên chức và người lao động thuộc 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 đảm bảo an toàn thông tin tại cơ quan; 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 cơ quan, của tỉnh, của các bộ ngành Trung ương.

c) Chịu trách nhiệm 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 mạo, các hành vi xâm phạm 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 ngăn chặn, xử lý.

d) Tham gia đầy đủ các chương trình phổ biến, bồi dưỡng về an toàn thông tin do cở quan và Sở Thông tin và Truyền thông phối hợp tổ chức (theo thành phần mời).

3. Trách nhiệm của các đối tượng khác:

a) Tuân thủ hướng dẫn, quy định về an toàn thông tin khi truy cập các hệ thống thông tin, đồng thời có trách nhiệm bảo vệ an toàn thông tin chung theo quy định.

b) Có trách nhiệm bảo vệ, quản lý tài khoản được cấp tạm thời (nếu có) để đăng nhập vào các hệ thống thông tin thực hiện giao dịch với các cơ quan qua các dịch vụ công trực tuyến, không giao tài khoản cho người khác sử dụng.

c) Khi phát hiện các nguy cơ mất an toàn hoặc hành vi xâm phạm an toàn thông tin trên các hệ thống thông tin báo ngay Trung tâm Công nghệ thông tin Tài nguyên và Môi trường.

Chương IV
KHEN THƯỞNG, XỬ LÝ VI PHẠM

Điều 12. Khen thưởng, xử lý vi phạm

1. Hàng năm trước ngày 25/10, Trung tâm Công nghệ thông tin Tài nguyên và Môi trường thực hiện khảo sát, đánh giá về công tác đảm bảo an toàn thông tin tại các phòng, đơn vị đề xuất xét khen thưởng các cá nhân, đơn vị theo quy định.

2. Tổ chức, cá nhân 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 khó khăn, vướng mắc, các phòng, đơn vị báo cáo về Lãnh đạo Sở *(qua Trung tâm Công nghệ thông tin Tài nguyên và Môi trường)* để tổng hợp, trình Giám đốc Sở xem xét, sửa đổi, bổ sung cho phù hợp./.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG
TỈNH KON TUM

Phạm Đức Hạnh