UBND TỈNH BÌNH ĐỊNH **SỞ XÂY DỰNG**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 279 /QĐ-SXD	*Bình Định, ngày 07 tháng 08 năm 2023*

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động Ứng dụng công nghệ thông tin của Sở Xây dựng

GIÁM ĐỐC SỞ XÂY DỰNG

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

Căn cứ Luật An toàn thông tin mạng ngày 16/11/2015;

Căn cứ Luật An ninh mạng ngày 12/6/2018;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về Bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 47/2020/NĐ-CP ngày 09/4/2020 của Chính phủ về việc Quản lý, kết nối và chia sẽ dữ liệu số của cơ quan nhà nước;

Căn cứ Quyết định số 22/2021/QĐ-UBND ngày 11/6/2021 của UBND tỉnh Bình Định về việc Ban hành Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Bình Định;

Căn cứ Quyết định số 91/2022/QĐ-UBND ngày 29/12/2022 của UBND tỉnh Bình Định Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Xây dựng;

Theo đề nghị của Chánh Văn phòng Sở.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Sở Xây dựng

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký và thay thế Quyết định số 284/QĐ-SXD ngày 27/11/2020 của Giám đốc Sở Xây dựng.

Điều 3. Chánh Văn phòng Sở, Chánh Thanh tra, Trưởng các phòng, ban, đơn vị thuộc Sở và công chức, viên chức và người lao động chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Lãnh đạo Sở;
- Lưu: VT, VP.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM SỞ XÂY DỰNG TỈNH BÌNH ĐỊNH

Trần Viết Bảo

UBND TỈNH BÌNH ĐỊNH
SỞ XÂY DỰNG

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

QUY CHẾ
Bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Sở Xây dựng

(Ban hành kèm theo Quyết định số:279 /QĐ-SXD ngày07 /08 /2023 của Giám đốc Sở Xây dựng)

CHƯƠNG I
NHỮNG QUY ĐỊNH CHUNG

Điều 1: Phạm vi điều chỉnh

Quy chế này quy định việc đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Sở Xây dựng.

Điều 2: Đối tượng áp dụng

a) Các phòng, ban, đơn vị (các phòng), công chức, viên chức và người lao động (CCVC&NLĐ) thuộc Sở Xây dựng.

b) Cơ quan, tổ chức, cá nhân có kết nối vào hệ thống thông tin của Sở.

c) Các quan, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin và an toàn thông tin mạng cho Sở.

Điều 3: Giải thích từ ngữ

1. *An toàn, an ninh thông tin* là sự bảo vệ thông tin, 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. *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, kết nối và trao đổi thông tin trên mạng nhằm phục vụ hoạt động của cơ quan, đơn vị.

4. *Xâm phạm an toàn, an ninh thông tin* 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. *Nguy cơ mất an toàn, an ninh thông tin* là những nhân tố chủ quan hoặc khách quan có khả năng ảnh hưởng tới trạng thái an toàn thông tin mạng.

6. *Sự cố an toàn, an ninh thông tin* 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.

7. *Đánh giá rủi ro an toàn, an ninh thông tin* là việc xác định, phân tích nguy cơ mất an toàn, an ninh thông tin có thể có và dự báo mức độ, phạm vi ảnh hưởng và khả năng gây thiệt hại khi xảy ra sự cố mất an toàn, an ninh thông tin.

8. *Quản rủi ro an toàn, an ninh thông tin* là việc thực hiện đánh giá rủi ro an toàn thông tin, xác định yêu cầu bảo vệ thông tin và hệ thống thông tin và áp dụng giải pháp phòng chống, giảm thiểu thiệt hại khi có sự cố mất an toàn thông tin.

9. *Phần mềm độc hại* là phần mềm có khả năng 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.

10. Hệ thống lọc phần mềm độc hại là tập hợp phần cứng, phần mềm được kết nối vào mạng để phát hiện, ngăn chặn, lọc và thống kê phần mềm độc hại.

Điều 4. Những hành vi bị nghiêm cấm

1. Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật An toàn thông tin

2. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập không dây của cá nhân vào mạng nội bộ; trên cùng một thiết bị thực hiện đồng thời truy cập vào mạng nội bộ và truy cập Internet bằng thiết bị kết nối Internet của cá nhân.

3. Tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin cài đặt trên thiết bị công nghệ thông tin phục vụ công việc; can thiệp thay đổi cấu hình, gỡ bỏ… các phần mềm đã cài đặt trên máy tính; tự ý thay thế, lắp mới, tráo đổi thành phần của máy tính phục vụ công việc.

Chương II

ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN TRONG THIẾT KẾ XÂY DỰNG HỆ THỐNG THÔNG TIN

Điều 5. Thiết kế, xây dựng hệ thống thông tin

1. Xây dựng các tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin, quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin.

2. Xây dựng các tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn, an ninh thông tin. Thiết lập các tường lửa (Firewall) để bảo vệ an toàn, an ninh thông tin. Đánh giá, phân loại cấp độ an toàn thông tin của hệ thống thông tin.

3. Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn, an ninh đặt ra đối với hệ thống.

Điều 6. Quản lý thuê dịch vụ, phát triển phần mềm

1. Khi thực hiện các hợp đồng liên quan đến việc thuê dịch vụ, phát triển phần mềm phải có điều khoản hoặc các cam kết an toàn, an ninh thông tin.

2. Trách nhiệm của cơ quan trong quá trình sử dụng dịch vụ công nghệ thông tin;

a) Quản lý thông tin, dữ liệu phát sinh từ dịch vụ đó, không để bên cung cấp dịch vụ truy nhập, sử dụng thông tin, dữ liệu thuộc phạm vi Nhà nước quản lý;

b) Yêu cầu bên cung cấp dịch vụ phải bảo mật thông tin, dữ liệu, mã nguồn, tài liệu thiết kế; triển khai các biện pháp bảo đảm an toàn thông tin theo quy định tại Quy chế này, Luật An toàn thông tin mạng và các quy định khác có liên quan;

c) Giám sát chặt chẽ và giới hạn quyền truy cập của bên cung cấp dịch vụ khi cho phép truy cập vào hệ thống thông tin của cơ quan, đơn vị.

3. Phần mềm phải được kiểm tra, đánh giá an toàn thông tin, kiểm thử trên môi trường thử nghiệm trước khi đưa vào hệ thống và vận hành sử dụng.

4. Tích hợp các phần mềm chống mã độc, phần mềm độc hại. Thường xuyên nâng cấp các phiên bản phần mềm, bản vá lỗ hổng mới nhất để hạn chế tối đa rủi ro mất an toàn hệ thống thông tin.

Điều 7. Thiết kế tài khoản, giám sát và sao lưu dự phòng

1. Khi thiết lập hệ thống mạng không dây (wireless LAN), cần thiết lập các thông số an toàn, quản lý tần số, phạm vi khu vực phát sóng và định kỳ thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật.

2. Quản lý đăng nhập hệ thống: Các hệ thống thông tin cần giới hạn số lần đăng nhập vào Hệ thống, tự động khoá tài khoản khi liên tục đăng nhập sai vượt quá số lần quy định.

3. Hệ thống thông tin, phần mềm, thiết bị mạng phải đảm bảo ghi nhận, lưu vết nhật ký sự kiện (logfile) của người quản trị và người dùng: quá trình đăng nhập hệ thống, các thao tác cấu hình hệ thống, quá trình truy xuất cập nhật, sửa chữa dữ liệu, quá trình sao lưu dự phòng… để theo dõi, xác định những sự kiện đã xảy ra của hệ thống.

Chương III

ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN MẠNG

Điều 8. Quản lý điều phối công tác an toàn, an ninh thông tin

1. Văn phòng Sở là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin (Sở Thông tin và Truyền thông, công an,…) trong việc phòng ngừa, .xử lý sự cố về an toàn, an ninh thông tin tại Sở.

2. Văn phòng Sở thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng tại Sở.

3. Phối hợp với các cơ quan liên quan trong công tác hỗ trợ, điều phối xử lý sự cố an toàn thông tin, ứng cứu các sự cố an toàn thông tin mạng.

Điều 9. Bảo đảm an toàn hạ tầng mạng

1. Quản lý hạ tầng mạng nội bộ

a) Đảm bảo tuân thủ các quy định kiến trúc hệ thống, tiêu chuẩn, quy chuẩn kỹ thuật; cài đặt, cấu hình, tổ chức hệ thống mạng phù hợp với các tiêu chuẩn ứng dụng công nghệ thông tin tại Sở Xây dựng, bảo đảm an toàn thông tin.

b) Tổ chức mô hình mạng: Cài đặt, cấu hình, tổ chức hệ thống mạng theo mô hình Máy khách/Máy chủ (Client/Server), hạn chế sử dụng mô hình mạng ngang hàng. Trang bị thiết bị tường lửa chuyên dụng hoặc phần mềm tường lửa để ngăn chặn và phát hiện xâm nhập trái phép vào mạng nội bộ của cơ quan khi kết nối với hệ thống bên ngoài.

c) Khi thực hiện truy nhập từ xa vào mạng nội bộ thực hiện chức năng quản trị, phải sử dụng giao thức mạng có mã hóa thông tin (như: SSL/TLS, VPN...) và thiết lập mật khẩu có độ phức tạp cao;

d) Không tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập không dây của cá nhân vào mạng nội bộ cơ quan.

e) Không tự ý thay đổi, gỡ bỏ biện pháp, giải pháp an toàn thông tin cài đặt trên thiết bị công nghệ thông tin phục vụ công việc; tự ý thay thế, lắp mới, tráo đổi thành phần của máy tính phục vụ công việc. Công chức phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng.

2. Quản lý hệ thống mạng không dây

a) Khi thiết lập mạng không dây để kết nối với mạng cục bộ thông qua các điểm truy nhập (Access Point - AP), gồm các tham số: Tên, mật khẩu có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặc biệt như: !, @, #, $, %), cấp phép truy nhập đối với địa chỉ vật lý (MAC Address), mã hóa dữ liệu theo cơ chế bảo mật WPA2 hoặc WPA3;

b) Mật khẩu đăng nhập phải được thiết lập có độ phức tạp cao, định kỳ 6 tháng thay đổi mật khẩu nhằm tăng cường công tác bảo mật;

c) Hạn chế cung cấp mật khẩu truy cập internet qua mạng không dây cho người không thuộc cơ quan khi không cần thiết.

Điều 10. Bảo đảm an toàn dữ liệu

1. Quản lý tài khoản và chữ ký số

a) Khi cấp tài khoản, chữ ký số lần đầu, người dùng phải thay đổi mật khẩu sau khi đăng nhập thành công.

b) Các hệ thống thông tin khi phân quyền phải thiết lập chế độ giới hạn số lần đăng nhập không hợp lệ vào hệ thống tối đa không quá 05 lần, khi người dùng đăng nhập sai vượt quá số lần quy định, tài khoản chuyển sang chế độ khóa quyền truy cập; các hệ thống thông tin xác lập chế độ thoát ra khỏi hệ thống nếu người sử dụng không tương tác trên hệ thống của phiên làm việc quá 10 phút;

c) Chủ tài khoản, chữ ký số không chia sẻ, giao quyền tài khoản, chữ ký số và mật khẩu truy nhập cho người khác. Không sử dụng tài khoản của người khác để đăng nhập vào hệ thống thông tin, cơ sở dữ liệu.

d) Tài khoản thư điện tử, chữ ký số chuyên dùng (xxx@sxd.binhdinh.gov.vn và chữ ký số do Ban Cơ yếu Chính phủ cấp) để phục vụ cho các hoạt động mang tính công vụ, không sử dụng để giao dịch, đăng ký trên mạng xã hội, các trang thông tin điện tử công cộng khác;

e) Công chức phụ trách công nghệ thông tin thực hiện việc quản trị, phân quyền, cấu hình các hệ thống được giao Sở quản lý, không sử dụng cùng một mật khẩu cho nhiều tài khoản khác nhau. Thực hiện điều chỉnh, thu hồi, hủy bỏ tài khoản, chữ ký số, chứng thư số, khi công chức thay đổi vị trí công tác, chuyển công tác, thôi việc, nghỉ hưu.

f) Công chức phụ trách công nghệ thông tin để 2. Cơ chế mã hóa và sao lưu dữ liệu phải đảm bảo tính toàn vẹn của dữ liệu.

3. Thiết lập sao lưu dự phòng ở mức vật lý cần thiết lập chức năng RAID (Redundant Arrays Of Inexpensive Disks hoặc Redundant Arrays of Independent Disks) để tăng tốc độ đọc ghi hoặc bảo đảm khả năng lưu trữ dự phòng.

4. Công chức phụ trách công nghệ thông tin phối hợp với các phòng thuộc Sở liên quan thực hiện xác định các thông tin, thực hiện quy trình sao lưu dự phòng và phục hồi cho các phần mềm, dữ liệu cần thiết theo quy định, quy trình sao lưu, lưu trữ hiện có.

5. Khi thực hiện chia sẻ tài nguyên trên máy tính, người sử dụng phải sử dụng mật khẩu để bảo vệ thông tin, dữ liệu; không thực hiện chia sẻ toàn bộ ổ cứng; theo dõi, giám sát để kết thúc chia sẻ tài nguyên ngay khi hoàn thành. Các thông tin, tài liệu, dữ liệu nhạy cảm phải được mã hóa trước khi trao đổi, truyền nhận qua mạng máy tính.

6. Khi cần mang máy tính đi bảo hành, bảo dưỡng, sửa chữa bên ngoài cơ quan, phải tháo rời bộ phận lưu trữ tài liệu khỏi thiết bị và để lại cơ quan, đơn vị hoặc trường hợp đặc biệt thì xóa dữ liệu lưu trữ trên thiết bị. Khi thanh lý thiết bị phải xóa dữ liệu lưu trữ bằng phần mềm hoặc thiết bị hủy dữ liệu chuyên dụng.

7. Thông tin, dữ liệu thuộc phạm vi bí mật Nhà nước phải được quản lý theo quy định hiện hành về bảo vệ bí mật Nhà nước.

Điều 11. Ứng cứu sự cố an toàn thông tin

1. Nguyên tắc ứng cứu xử lý sự cố

a) Chủ động, kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả;

b) Phối hợp chặt chẽ, tuân thủ quy định của pháp luật về điều phối ứng cứu sự cố an toàn thông tin;

c) Ứng cứu xử lý sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản hệ thống thông tin;

d) Việc xử lý sự cố an toàn thông tin phải bảo đảm quyền và lợi ích hợp pháp của cơ quan, đơn vị; cá nhân, bảo mật thông tin cá nhân, thông tin riêng của cơ quan, đơn vị khi tham gia các hoạt động ứng cứu xử lý sự cố

2. Quy trình phối hợp ứng cứu xử lý sự cố

a) Bước 1: Nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc thẩm quyền cơ quan trực tiếp quản lý thì thực hiện tiếp Bước 2. Nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc Trung tâm Công nghệ thông tin và Truyền thông trực thuộc Sở Thông tin và Truyền thông quản lý (các hệ thống được triển khai tập trung tại Trung tâm tích hợp Dữ liệu tỉnh) thì thực hiện tiếp Bước 3;

b) Bước 2: Tiến hành xử lý sự cố, nếu sự cố được khắc phục thì lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố. Khi sự cố vượt quá khả năng xử lý của cơ quan lập biên bản ghi nhận và thực hiện tiếp Bước 3;

c) Bước 3: Báo sự cố về Trung tâm Công nghệ thông tin và Truyền thông theo mẫu số 01 được quy định tại Quyết định số 22/2021/QĐ-UBND ngày 11/6/2021 của UBND tỉnh Bình Định.

d) Bước 4: Phối hợp với Trung tâm Công nghệ thông tin và Truyền thông và các cơ quan có liên quan để tiến hành khắc phục sự cố và thực hiện tiếp Bước 5;

e) Bước 5: Lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố theo mẫu số 02 được quy định tại Quyết định số 22/2021/QĐ-UBND ngày 11/6/2021 của UBND tỉnh Bình Định.

3. Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của cơ quan; Lãnh đạo cơ quan 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.

4. Công chức chuyên trách về an toàn thông tin có trách nhiệm

a) Xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng, ứng phó sự cố an toàn thông tin mạng.

b) Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định.

c) Phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin; Yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống.

Chương IV
TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG VÀ TỔ CHỨC THỰC HIỆN

Điều 12. Trách nhiệm của Văn phòng Sở

1. Tham mưu Lãnh đạo Sở về công tác bảo đảm an toàn thông tin và chịu trách nhiệm trước Lãnh đạo Sở trong việc bảo đảm an toàn thông tin tại cơ quan.

2. Tham mưu Lãnh đạo Sở xây dựng, bổ sung (nếu có thay đổi) hồ sơ đề xuất cấp độ an toàn thông tin và bảo đảm an toàn cho các hệ thống thông tin theo quy định của Luật An toàn thông tin mạng và các văn bản hướng dẫn thi hành Luật An toàn thông tin mạng

3. Đầu mối thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trong cơ quan. Chủ trì, phối hợp với các cơ quan, đơn vị có liên quan tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hàng năm.

4. Hàng năm, đề xuất Lãnh đạo Sở cử công chức tham gia các lớp đào tạo, tập huấn về công tác bảo đảm an toàn thông tin mạng. Tổ chức tuyên truyền về an toàn thông tin mạng trong công tác quản lý.

5. Tham mưu Lãnh đạo Sở phối hợp với Công an tỉnh, Sở Thông tin và Truyền thông và các cơ quan có liên quan có các biện pháp phòng, chống các thông tin vi phạm pháp luật, ảnh hưởng đến an ninh quốc gia, trật tự, an toàn xã hội trên môi trường mạng, nhất là trên các cổng/trang thông tin điện tử Sở Xây dựng.

6. Hằng năm xây dựng dự toán kinh phí cho việc ứng dụng công nghệ thông tin nói chung và công tác đảm bảo an toàn thông tin mạng nói riêng tại Sở Xây dựng; lập kế hoạch nâng cấp, bảo trì, sửa chữa, gia hạn bản quyền phần mền… cho các hệ thống phần cứng, phần mền nhằm thực hiện tốt công tác bảo mật, bảo đảm an toàn thông tin mạng đưa vào dự toán chi năm sau để triển khai thực hiện.

Điều 13. Trách nhiệm của cơ quan, đơn vị thuộc Sở.

1. Giám đốc Sở, Trung tâm có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trong công tác bảo đảm an toàn thông tin mạng của cơ quan, đơn vị.

2. Phân công CCVC&NLĐ phụ trách công nghệ thông tin bảo đảm an toàn thông tin của cơ quan, chỉ đạo CCVC&NLĐ nghiêm túc chấp hành các quy định về bảo đảm an toàn thông tin; thường xuyên tổ chức quán triệt các quy định về an toàn thông tin trong cơ quan, đơn vị.

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

4. Phối hợp chặt chẽ với Công an tỉnh, Sở Thông tin và Truyền thông và các cơ quan, đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin trên không gian mạng.

Điều 14. Trách nhiệm của công chức, viên chức và người lao động.

1. Trách nhiệm của công chức, viên chức phụ trách về an toàn thông tin/công nghệ thông tin:

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

b) Thực hiện việc giám sát, đánh giá, báo cáo Người đứng đầu các rủi ro mất an toàn thông tin mạng và mức độ nghiêm trọng của các rủi ro đó.

c) Phối hợp với các tổ chức, cá nhân có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn thông tin mạng.

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

2. Trách nhiệm của người sử dụng

a) Nghiêm túc chấp hành Quy chế này và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao.

b) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng.

c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý.

d) Tham gia đầy đủ các chương trình bồi dưỡng, tập huấn về an toàn thông tin mạng khi được phân công.

Điều 15. Tổ chức thực hiện

1. Công chức, viên chức, người lao động tại các phòng, đơn vị trực thuộc Sở có trách nhiệm tổ chức triển khai thực hiện Quy chế này.

2. Giao Văn phòng Sở theo dõi, triển khai việc thực hiện Quy chế này, có trách nhiệm cài đặt, quản lý các phần mềm hệ thống và phần mềm ứng dụng trong hệ thống mạng máy tính tại Sở; Nghiên cứu, đề xuất, nâng cấp công nghệ, phần mềm theo định hướng quản lý nhà nước của ngành và tuân theo quy định của Nhà nước.

3. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc cần phản ánh kịp thời về Sở (qua Văn phòng Sở) để tổng hợp báo cáo Giám đốc Sở xem xét quyết định điều chỉnh, bổ sung cho phù hợp./.