Số: 222/QĐ-SNV
Thời gian ký: 12/05/2022 14:54:24 +07:00

UBND TỈNH BÌNH ĐỊNH
SỞ NỘI VỤ

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

QUY CHẾ
Đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Sở Nội vụ Bình Định

(Ban hành kèm theo Quyết định số: 222 /QĐ-SNV ngày 12/05/2022 của Sở Nội vụ)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh, đối tượng áp dụng

1. Quy chế này quy định các hoạt động thực hiện bảo đảm an toàn thông tin các hệ thống thông tin trong hoạt động của Sở Nội vụ.

2. Quy chế này áp dụng đối với các cơ quan, đơn vị thuộc, trực thuộc Sở và công chức, viên chức, người lao động thuộc Sở Nội vụ.

Điều 2. Giải thích từ ngữ

1. An toàn thông tin mạng: Là công tác 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 nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

2. 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 của một cơ quan, tổ chức.

3. 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 của thông tin.

4. 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.

Điều 3. Nguyên tắc bảo đảm an toàn thông tin

1. Hoạt động an toàn thông tin mạng phải đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước, giữ vững ổn định chính trị, trật tự, an toàn xã hội và thúc đẩy phát triển kinh tế - xã hội.

2. Công chức, viên chức, người lao động Sở Nội vụ không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác.

3. Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức.

4. Hoạt động an toàn thông tin mạng phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.

Chương II
QUY ĐỊNH ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 4. Bảo vệ bí mật nhà nước liên quan an toàn thông tin mạng

1. Quy định về soạn thảo, in ấn, phát hành và sao chụp tài liệu mật

a) Không được sử dụng máy tính nối mạng internet để soạn thảo văn bản, chuyển giao, lưu trữ thông tin có nội dung thuộc bí mật nhà nước; cung cấp tin, tài liệu và đưa thông tin bí mật nhà nước trên Trang thông tin điện tử (Trang TTĐT) Sở Nội vụ và các trang mạng khác.

b) Không được in, sao chụp tài liệu bí mật nhà nước trên các thiết bị kết nối mạng internet.

c) Bố trí 01 máy vi tính riêng, không kết nối mạng nội bộ và mạng internet dùng để quản lý, sử dụng soạn thảo các tài liệu mật của nhà nước theo quy định.

2. Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật, các cơ quan, đơn vị phải báo cáo cho người có thẩm quyền. Không được tự ý cho phép các tổ chức, cá nhân không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố.

3. Trước khi thanh lý các máy tính trong cơ quan, đơn vị, công chức, viên chức phụ trách công nghệ thông tin dùng các biện pháp kỹ thuật xoá bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

Điều 5. Cấp phát, thu hồi, cập nhật và quản lý các tài khoản truy cập vào hệ thống thông tin

1. Việc tạo tài khoản, cấp quyền truy cập, đăng nhập hệ thống thông tin phải đảm bảo mỗi tài khoản phải gắn với người sử dụng và không được trung lặp. Trường hợp sử dụng tài khoản dùng chung cho một nhóm người hay một cơ quan, đơn vị, phải quy định, phân công cụ thể cá nhân đại diện có trách nhiệm quản lý tài khoản. Người dùng chỉ được truy cập các thông tin phù hợp với nhiệm vụ, chức trách được giao và có trách nhiệm bảo mật tài khoản truy cập được cấp.

2. Công chức, viên chức phụ trách công nghệ thông tin thực hiện quản lý, cấp tài khoản cá nhân và phân quyền truy cập cho người sử dụng trên tất cả các hệ thống thông tin sử dụng sau khi có ý kiến đồng ý của người đứng đầu cơ quan, đơn vị. Thực hiện hủy tài khoản truy cập cá nhân và ngắt kết nối đối với các hành vi cố ý tấn công hoặc gây trở ngại cho mạng máy tính và các trường hợp không còn làm việc tại cơ quan, đơn vị thuộc và trực thuộc Sở. Hướng dẫn người sử dụng thay đổi mật khẩu ngay sau khi đăng nhập lần đầu tiên và bảo vệ thông tin của tài khoản theo quy định.

3. Việc cài đặt, thiết lập mật mã đăng nhập, truy cập hệ thống thông tin phải có độ phức tạp cao, khó đoán và bảo mật (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặc biệt như: !, @, #, $, %,...).

Điều 6. 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 cơ quan Sở Nội vụ, 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, đơn vị 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, đơn vị.

đ) 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, thay đổi thành phần của máy tính phục vụ công việc. Công chức, viên chức, người lao động 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, đơn vị khi không cần thiết.

Điều 7. Bảo đảm an toàn dữ liệu

1. Quản lý tài khoản và chữ ký số

a) Khi được 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 (có dạng abc@snv.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; định kỳ 01 năm kiểm tra việc lưu trữ của hệ thống thư điện tử, tiến hành xóa các mail quá cũ, không cần thiết để đảm bảo hệ thống hoạt động ổn định thông suốt.

đ) Tài khoản quản trị hệ thống được giao cho công chức, viên chức phụ trách công nghệ thông tin phục vụ cho công tác quản trị, phân quyền, cấu hình hệ thống đó. Công chức, viên chức quản trị hệ thống không sử dụng cùng một mật khẩu cho nhiều tài khoản khác nhau.

e) Khi cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc, nghỉ hưu, ngay từ thời điểm Quyết định có hiệu lực, cơ quan, đơn vị quản lý cá nhân đó phải thông báo cho cơ quan, đơn vị vận hành (Văn phòng Sở) để điều chỉnh, thu hồi, hủy bỏ tài khoản, chữ ký số, chứng thư số.

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, viên chức phụ trách công nghệ thông tin phối hợp với các đơn vị có 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, đơn vị phải tháo rời bộ phận lưu trữ tài liệu (HDD) 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 8. Ứng cứu sự cố an toàn thông tin

1. 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, đơn vị 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, đơn vị, lập biên bản ghi nhận và thực hiện tiếp Bước 3.

c) Bước 3: Báo sự cố đến Sở Thông tin và Truyền thông theo Mẫu số 01 được quy định tại Quyết định số 22/2021/QĐ-UBND ngày 11 tháng 6 năm 2021.

d) Bước 4: Phối hợp với Trung tâm Công nghệ thông tin và Truyền thông trực thuộc Sở Thông tin và Truyền thông và các cơ quan, đơn vị có liên quan để tiến hành khắc phục sự cố và thực hiện tiếp Bước 5.

đ) 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 tháng 6 năm 2021.

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

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

Điều 9. Trách nhiệm của Văn phòng Sở

1. Tham mưu, đề xuất Giám đốc Sở công tác bảo đảm an toàn thông tin tại Sở Nội vụ và chịu trách nhiệm trước Giám đốc Sở trong việc bảo đảm an toàn thông tin tại cơ quan.

2. Chủ trì, phối hợp với các cơ quan, đơn vị trực thuộc Sở tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hằng năm.

3. Hằng năm, đề xuất Giám đốc Sở cử công chức, viên chức phụ trách công nghệ thông tin của các cơ quan, đơn vị bồi dưỡng, tập huấn về công tác

bảo đảm an toàn thông tin mạng, tham dự các hội nghị, hội thảo chuyên đề về an toàn thông tin mạng do các cơ quan liên quan tổ chức.

4. 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 Trang TTĐT Sở Nội vụ.

5. Là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin; tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng tại Sở Nội vụ.

6. Hằng năm xây dựng dự toán kinh phí cho việc ứng dụng công nghệ thông tin nói chung và công tác bảo đảm an toàn thông tin mạng nói riêng tại Sở Nội vụ; lập kế hoạch nâng cấp, bảo trì, sửa chữa, gia hạn bản quyền phần mềm... cho các hệ thống phần cứng, phần mềm 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 10. Trách nhiệm của các cơ quan, đơn vị thuộc và trực thuộc Sở

1. Người đứng đầu các cơ quan, đơn vị thuộc và trực thuộc Sở 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 mình.

2. Phân công công chức, viên chức phụ trách công nghệ thông tin bảo đảm an toàn thông tin của cơ quan, đơn vị; chỉ đạo công chức, viên chức và người lao động nghiêm túc chấp hành các quy định về bảo đảm an toàn thông tin; tạo điều kiện để các công chức, viên chức phụ trách công nghệ thông tin được học tập, nâng cao trình độ về 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 cơ quan, 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 11. 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 tại cơ quan, đơn vị

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 cơ quan, đơn vị 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 cơ quan, 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 12. Tổ chức thực hiện

1. Căn cứ Quy chế này, Người đứng đầu các cơ quan, đơn vị thuộc và 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. Định kỳ tổng hợp báo cáo Giám đốc Sở tình hình thực hiện đảm bảo an toàn thông tin mạng tại các cơ quan, đơn vị theo quy định.

3. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc các cơ quan, đơn vị tổng hợp phản ánh gửi về Sở (qua Văn phòng Sở), trình Giám đốc Sở xem xét, sửa đổi bổ sung cho phù hợp./.