UBND TỈNH BÌNH ĐỊNH **SỞ NGOẠI VỤ**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 816 /QĐ-SNgV	*Bình Định, ngày 30 tháng 9 năm 2021*

QUYẾT ĐỊNH
Về việc ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Sở Ngoại vụ tỉnh Bình Định

GIÁM ĐỐC SỞ NGOẠI VỤ TỈNH BÌNH ĐỊNH

Căn cứ Quyết định số 3830/QĐ-UBND ngày 27/10/2015 của UBND tỉnh Bình Định quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Ngoại vụ tỉnh Bình Định;

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

Theo đề nghị của Chánh Văn phòng.

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 Ngoại vụ tỉnh Bình Định.

Điều 2. Giao Văn phòng Sở có trách nhiệm phổ biến triển khai Quy chế này đến các phòng, đơn vị thuộc sở và theo dõi việc thực hiện của các đơn vị nêu trên; kịp thời báo cáo đề xuất Giám đốc Sở các nội dung liên quan theo quy định tại Quy chế này.

Điều 3. Quyết định này thay thế Quyết định số 816/QĐ-SNgV ngày 24/10/2014 của Sở Ngoại vụ.

Chánh Văn phòng, Trưởng các Phòng thuộc Sở và công chức liên quan chịu trách nhiệm thi hành Quyết định này kể từ ngày ký./.

Nơi nhận: - Như Điều 3; - Sở TT&TT; - Lãnh đạo Sở; - Lưu: VT, VP.	**GIÁM ĐỐC**  **Nguyễn Thái Bình**

Số: 816/QĐ-SNgV
Thời gian ký: 30/09/2021 09:00:03 +07:00

UBND TỈNH BÌNH ĐỊNH
SỞ NGOẠI VỤ

CỘNG HÒA 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 Ngoại vụ tỉnh Bình Định

(*Ban hành kèm theo Quyết định số: /QĐ-SNgV ngày tháng 9 năm 2021 của Sở Ngoại vụ tỉnh Bình Định)*

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định nội dung, biện pháp nhằm bảo đảm an toàn thông tin thuộc hệ thống thông tin trong hoạt động ứng dụng công nghệ thông tin (sau đây gọi tắt là CNTT) phục vụ công tác quản lý và chỉ đạo điều hành của Sở Ngoại vụ tỉnh Bình Định.

Điều 2. Đối tượng áp dụng

Quy chế này áp dụng với tất cả các phòng, đơn vị, công chức và người lao động thuộc Sở.

Điều 3. Giải thích từ ngữ

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

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 cơ quan, đơn vị.

3. *Chủ quản hệ thống thông tin*: Là cơ quan Sở Ngoại vụ có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin của Sở Ngoại vụ.

4. *Đơn vị vận hành hệ thống thông tin*: Là đơn vị được chủ quản hệ thống thông tin (Sở Ngoại vụ) giao nhiệm vụ vận hành hệ thống thông tin. Trường hợp Sở Ngoại vụ thuê ngoài dịch vụ công nghệ thông tin, đơn vị vận hành hệ thống thông tin là bên cung cấp dịch vụ.

5. *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.

6. *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.

7. *Mạng ngang hàng:* Là mô hình mạng mà trong đó các máy tính có quyền bình đẳng như nhau, mỗi máy tính có quyền chia sẻ tài nguyên và sử dụng các tài nguyên từ máy tính khác.

8. *Đơn vị chuyên trách về công nghệ thông tin và an toàn thông tin:* Là đơn vị chuyên trách về công nghệ thông tin của Sở Ngoại vụ hoặc do Sở chỉ định/thuê, có chức năng, nhiệm vụ bảo đảm an toàn thông tin của Sở Ngoại vụ.

9. *Cán bộ chuyên trách:* Là công chức được giao phụ trách an toàn thông tin/công nghệ thông tin tại cơ quan, trực tiếp tham mưu lãnh đạo Sở khai thác, quản lý và thực hiện công tác ứng dụng CNTT tại cơ quan, đơn vị, bảo đảm kỹ thuật và an toàn, an ninh thông tin cho việc khai thác, vận hành hệ thống CNTT tại đơn vị.

Điều 4. Nguyên tắc bảo đảm an toàn thông tin

1. Trưởng các phòng, đơn vị, công chức và người lao động thuộc Sở có trách nhiệm bảo đảm an toàn thông tin mạng. Hoạt động an toàn thông tin mạng của cơ quan, cá nhân 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. Các phòng, đơn vị, công chức thuộc Sở 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 5. Yêu cầu thiết kế, xây dựng hệ thống thông tin

1. Khi thiết kế xây dựng, nâng cấp, mở rộng hệ thống thông tin (nếu có), Sở phải xây dựng phương án bảo đảm an toàn thông tin trong hồ sơ thiết kế và gửi Sở Thông tin và Truyền thông thẩm định trước khi trình cấp có thẩm quyền phê duyệt dự án.

2. Đánh giá, phân loại cấp độ an toàn thông tin của hệ thống thông tin

a) Sở Ngoại vụ có trách nhiệm tổ chức đánh giá, phân loại cấp độ an toàn thông tin của hệ thống thông tin theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống theo cấp độ (gọi tắt là Nghị định số 85/2016/NĐ-CP) để áp dụng phương án bảo đảm an toàn thông tin phù hợp;

b) Hồ sơ đề xuất cấp độ bao gồm các tài liệu được quy định tại Điều 15 Nghị định số 85/2016/NĐ-CP, gửi Sở Thông tin và Truyền thông thẩm định, trình cấp có thẩm quyền phê duyệt.

3. Trước khi đưa vào vận hành, khai thác hệ thống thông tin, Sở Ngoại vụ phải thực hiện kiểm thử hoặc vận hành thử trước khi đưa vào sử dụng. Kết quả kiểm thử, vận hành thử phải được lập thành văn bản và tuân thủ theo quy định tại Điều 10 Thông tư số 24/2020/TT-BTTTT ngày 09/9/2020 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về công tác triển khai, giám sát công tác triển khai và nghiệm thu dự án đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước.

Điều 6. Quản lý thuê dịch vụ công nghệ thông tin

1. Trong trường hợp ký kết hợp đồng thuê dịch vụ công nghệ thông tin, Sở Ngoại vụ phải xác định rõ phạm vi, trách nhiệm, quyền hạn và nghĩa vụ của các bên về bảo đảm an toàn thông tin. Trong hợp đồng phải bao gồm các điều khoản về việc xử lý vi phạm quy định bảo đảm an toàn thông tin và trách nhiệm bồi thường thiệt hại do hành vi vi phạm của bên cung cấp dịch vụ gây ra.

2. Trách nhiệm của Sở Ngoại vụ 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 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 Sở Ngoại vụ.

3. Trách nhiệm của Sở Ngoại vụ khi phát hiện bên cung cấp dịch vụ có dấu hiệu vi phạm quy định bảo đảm an toàn thông tin

a) Tạm dừng hoặc đình chỉ hoạt động của bên cung cấp dịch vụ tùy theo mức độ vi phạm;

b) Thông báo chính thức các hành vi vi phạm của bên cung cấp dịch vụ;

c) Thu hồi ngay lập tức quyền truy cập hệ thống thông tin đã cấp cho bên cung cấp dịch vụ;

d) Kiểm tra, xác định, lập báo cáo mức độ vi phạm và thiệt hại xảy ra; thông báo cho bên cung cấp dịch vụ và tiến hành các thủ tục xử lý vi phạm và bồi thường thiệt hại…

4. Trách nhiệm của Sở Ngoại vụ khi kết thúc sử dụng dịch vụ

a) Thu hồi quyền truy cập hệ thống thông tin và các tài sản khác liên quan đã cấp cho bên cung cấp dịch vụ; thay đổi các khóa, mật khẩu truy cập hệ thống thông tin;

b) Yêu cầu bên cung cấp dịch vụ chuyển giao đầy đủ các thông tin, dữ liệu, mã nguồn, tài liệu thiết kế và các công cụ cần thiết để bảo đảm cơ quan, đơn vị vẫn có thể khai thác sử dụng dịch vụ được liên tục kể cả trong trường hợp thay đổi bên cung cấp dịch vụ.

Điều 7. Bảo vệ bí mật nhà nước trong hoạt động ứng dụng công nghệ thông tin

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 của Sở;

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

c) Phải bố trí 01 máy vi tính riêng, không kết nối mạng nội bộ và mạng Internet dùng để quản lý, 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 phòng, đơn vị phải báo cáo cho Giám đốc Sở (qua Văn phòng Sở). Không được cho phép các tổ chức, cá nhân không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố của máy tính.

3. Trước khi thanh lý các máy tính của cơ quan, cán bộ chuyên trách công nghệ thông tin của Sở phải dùng các biện pháp kỹ thuật xoá bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

Điều 8. Quy định về cấp phát, thu hồi, cập nhật và quản lý các tài khoản truy cập vào hệ thống thông tin

1. Trách nhiệm, quyền hạn của công chức thuộc Sở khi truy cập, đăng nhập các hệ thống thông tin, đảm bảo mỗi người dùng khi sử dụng hệ thống thông tin phải được cấp và sử dụng tài khoản truy cập với định danh duy nhất gắn với người dùng. Trường hợp sử dụng tài khoản dùng chung cho một nhóm người hay một đơn vị, phải có cơ chế xác định các cá nhân, đơn vị có trách nhiệm quản lý tài khoản. Người dùng chỉ được truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình và có trách nhiệm bảo mật tài khoản truy cập được cấp.

2. Cán bộ chuyên trách CNTT của Sở thực hiện quản lý, cấp tài khoản cá nhân và phân quyền truy cập cho người sử dụng trên tất cả các máy trạm đặt tại Sở Ngoại vụ. Trong trường hợp cần thiết có thể 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; hủy quyền truy cập hệ thống thông tin đối với công chức nghỉ chế độ, chuyển công tác và đảm bảo khả năng vẫn truy nhập được vào các hồ sơ được tạo ra bởi công chức đó. 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. Mật mã đăng nhập, truy cập hệ thống thông tin phải 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 !, @, #, $, %,...).

Điều 9. Bảo đảm nguồn nhân lực

1. Cán bộ chuyên trách được tuyển dụng vào vị trí công việc an toàn thông tin phải có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng.

2. Cán bộ chuyên trách được đảm bảo các điều kiện học tập, tiếp cận công nghệ, kiến thức an toàn bảo mật thông tin trước khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ.

3. Cán bộ được giao nhiệm vụ quản lý, vận hành truy cập, khai thác đối với các hệ thống thông tin thực hiện theo trách nhiệm và phân quyền được quy định; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài; theo dõi và phát hiện các trường hợp truy cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, báo cáo cho Giám đốc Sở biết và tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm.

4. Thường xuyên tổ chức, phổ biến các quy định về đảm bảo an toàn thông tin, nhằm nâng cao nhận thức về trách nhiệm đảm bảo an toàn thông tin cho các đơn vị, công chức thuộc Sở sử dụng hệ thống thông tin do Sở Ngoại vụ quản lý.

Điều 10. Bảo đảm an toàn hạ tầng mạng

1. Quản lý hạ tầng mạng nội bộ

a) 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 của các cơ quan nhà nước, bảo đảm an toàn thông tin; hạn chế sử dụng mô hình mạng có nguy cơ mất an toàn thông tin cao;

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; Xây dựng hoặc thuê hệ thống giám sát an toàn thông tin để kiểm soát, phát hiện truy cập trái phép vào hệ thống.

c) Đối với các phòng, đơn vị trực thuộc không nằm cùng một khu vực thì cần thiết lập mạng riêng ảo (VPN) để tăng cường an ninh cho hạ tầng mạng nội bộ. Khi thiết lập các dịch vụ trên môi trường mạng Internet, chỉ cung cấp những chức năng thiết yếu nhất nhằm bảo đảm duy trì hoạt động của hệ thống thông tin; hạn chế sử dụng/mở cổng giao tiếp mạng, giao thức và các dịch vụ không cần thiết.

d) 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..

đ) Xây dựng quy trình kết nối thiết bị đầu cuối của người sử dụng vào hệ thống mạng; truy nhập và quản lý cấu hình hệ thống; cấu hình tối ưu, tăng cường bảo mật cho thiết bị mạng, bảo mật trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác.

e) 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.

g) 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 của Sở 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), đơn vị vận hành phải thiết lập các tham số: Tên, nhận dạng dịch vụ (Service Set Identifier - SSID), 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) Khi cung cấp truy cập Internet qua mạng không dây cho người ngoài, cơ quan, đơn vị vận hành phải tạo thêm một SSID riêng và giới hạn băng thông truy cập phù hợp đối với đối tượng này.

Điều 11. Bảo đảm an toàn máy chủ và ứng dụng

1. Trên hệ thống máy chủ

a) Hệ điều hành được cài đặt là phần mềm có bản quyền (bao gồm bản quyền thương mại hoặc mã nguồn mở có nguồn gốc rõ ràng), các dịch vụ cài đặt trên máy chủ là các dịch vụ được sử dụng dùng chung cho cơ quan, không cài đặt các dịch vụ không sử dụng;

b) Thiết lập chế độ tự động cập nhật phiên bản và hệ điều hành, phần mềm, ứng dụng và hệ quản trị cơ sở dữ liệu được cài đặt trên máy chủ, phải thiết lập mật

khẩu truy nhập chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng đối với tất cả máy chủ;

c) Các máy chủ cần được cài đặt mật khẩu ở phần cấu hình (setup) của BIOS (Basic Input/Output System), trong đó lưu ý việc vô hiệu hóa các cổng USB trên máy chủ.

2. Sở Ngoại vụ có trách nhiệm trang bị phần mềm phòng chống mã độc (antivirus) có bản quyền cho hệ thống máy chủ; thiết lập chế độ tự động cập nhật phiên bản mới, các bản vá lỗi; chế độ tự động quét mã độc khi sao chép, mở các tập tin; chế độ quét toàn bộ máy tính định kỳ hằng tuần.

3. Định kỳ hằng tuần, cán bộ chuyên trách CNTT của Sở phải kiểm tra các tiến trình trên máy chủ nhằm sớm phát hiện nguy cơ cài cắm phần mềm độc hại trên máy chủ.

4. Quản lý tệp tin lưu trữ sự kiện (logfile): Cán bộ chuyên trách CNTT của Sở phải thường xuyên kiểm tra, quản lý, sao lưu các logfile theo từng tháng, thời gian lưu trữ logfile trên máy chủ và thiết bị từ 06 - 12 tháng, các tập tin logfile cũ trong 03 năm trước đó cần được lưu trữ trên các ổ cứng ngoài; định kỳ 06 tháng kiểm tra, bảo đảm tính toàn vẹn của các logfile, hạn chế tình trạng tràn logfile gây ảnh hưởng đến hoạt động của hệ thống thông tin.

5. Quản lý lưu ký hệ thống: Việc thực hiện lưu ký hệ thống thông tin (nếu có), Sở Ngoại vụ yêu cầu cơ quan, đơn vị cung cấp dịch vụ lưu ký phải tổ chức máy chủ cơ sở dữ liệu và máy chủ ứng dụng nằm trên hai máy chủ khác nhau và được bảo vệ bởi lớp bảo vệ bao gồm: Tường lửa, thiết bị phòng chống tấn công từ chối dịch vụ DDoS (Distributed Denial of Service), thiết bị phát hiện và phòng chống xâm nhập trái phép (IPS/IDS);

6. Quản lý phiên bản: cán bộ chuyên trách CNTT của Sở phải xây dựng nhật ký quản lý phiên bản hệ thống thông tin bao gồm các thông tin: Chủ đầu tư, tên hệ thống thông tin, đơn vị phát triển, tên phiên bản; các chức năng của phiên bản; các chức năng thay đổi so với phiên bản trước, thời gian thay đổi; lưu trữ các phiên bản hệ thống thông tin tại hệ thống lưu trữ độc lập;

7. Khi thiết lập cung cấp các dịch vụ ra môi trường mạng (tuân thủ theo TCP/UDP Port), Sở Ngoại vụ yêu cầu nhà cung cấp dịch vụ cấu hình trên máy chủ ứng dụng những dịch vụ thiết yếu nhất để bảo đảm hoạt động của hệ thống, không

kích hoạt những chức năng, cổng giao tiếp mạng, giao thức và các dịch vụ không sử dụng (không thiết lập cấu hình các dịch vụ ra môi trường mạng đối với máy chủ cơ sở dữ liệu).

Điều 12. 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 cho người dùng truy nhập, cơ quan, đơn vị vận hành phải thông báo (qua email, điện thoại) và người dùng phải thay đổi mật khẩu sau khi đăng nhập thành công lần đầu;

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 (ví dụ tài khoản thư điện tử, chữ ký số, chứng thư số) để đăng nhập vào hệ thống thông tin, cơ sở dữ liệu;

d) Tài khoản thư điện tử, chữ ký số chuyên dùng (xxx@songoaivu.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 cán bộ chuyên trách công nghệ thông tin phục vụ cho công tác quản trị, phân quyền, cấu hình hệ thống đó. Cán bộ chuyên trách 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 quản lý cá nhân đó phải thông báo cho Sở Thông tin và Truyền thông 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. Các cơ quan, đơn vị khi triển khai dịch vụ 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. Trong trường hợp, Sở Ngoại vụ thuê dịch vụ cần yêu cầu nhà cung cấp dịch vụ thiết lập các giải pháp sao lưu tự động đối với dữ liệu trên máy chủ cơ sở dữ liệu và máy chủ ứng dụng và xây dựng các kịch bản có sẵn để khôi phục lại toàn bộ máy chủ hoặc các tập tin, thư mục khi xảy ra sự cố.

4. Đối với công tác sao lưu dự phòng và khôi phục dữ liệu (tần suất sao lưu dự phòng, phương tiện lưu trữ, thời gian lưu trữ; nơi lưu trữ, phương thức lưu trữ và phương thức lấy dữ liệu ra khỏi phương tiện lưu trữ)

a) Lập danh sách các dữ liệu, phần mềm cần được sao lưu, có phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu;

b) Xây dựng tài liệu, quy trình hướng dẫn sao lưu/phục hồi dữ liệu của hệ thống: Đơn vị quản trị hệ thống thực hiện xây dựng Tài liệu hướng dẫn sao lưu cụ thể đối với từng hệ thống cung cấp dịch vụ, hệ thống điều hành mà Sở Ngoại vụ quản lý.

5. Cán bộ chuyên trách CNTT của Sở 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 các phần mềm, dữ liệu cần thiết theo quy định, hoặc theo quy trình sao lưu, lưu trữ hiện có. Các nội dung thực hiện gồm: lập danh sách các dữ liệu (thông tin cấu hình của mạng, máy chủ), phần mềm ứng dụng, cơ sở dữ liệu, tệp tin ghi nhật ký hệ được sao lưu, có phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu; thực hiện quy trình sao lưu dự phòng và phục hồi.

6. Dữ liệu sao lưu phải được lưu trữ an toàn trên Hệ thống lưu trữ dự phòng, thiết bị lưu trữ ngoài và được kiểm tra thường xuyên đảm bảo sẵn sàng cho việc sử dụng khi cần; việc kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu tối thiểu 6 tháng một lần (hoặc khi có yêu cầu đột xuất).

7. Các tên miền (bao gồm cả tên miền *.binhdinh.gov.vn) khi không còn sử dụng, Sở Ngoại vụ có văn bản gửi đến Sở Thông tin và Truyền thông và Trung Tâm Internet Việt Nam (VNNIC) để đề nghị hủy tên miền; các hệ thống thông tin không sử dụng, chủ quản hệ thống thông tin thực hiện việc thu hồi máy chủ, thu

hồi ứng dụng và thực hiện việc lưu trữ dữ liệu ra thiết bị lưu trữ ngoài và yêu cầu cơ quan, đơn vị cung cấp dịch vụ lưu ký xóa hoàn toàn dữ liệu trên các máy chủ.

8. Khi thực hiện chia sẻ tài nguyên trên máy chủ hoặc máy trạm, đơn vị vận hành (do Sở Ngoại vụ thuê) 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.

9. Cơ quan quản lý máy chủ, máy trạm và thiết bị lưu trữ khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài cơ quan, đơn vị phải tháo rời bộ phận lưu trữ khỏi thiết bị và để lại cơ quan, đơn vị hoặc 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.

10. 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 13. Bảo đảm an toàn thiết bị đầu cuối

1. Trên máy tính cá nhân phải thiết lập chế độ tự động cập nhật hệ điều hành trên máy tính, phải thiết lập mật khẩu truy nhập chế độ tự động bảo vệ màn hình khi không sử dụng; sử dụng những trình duyệt an toàn, đáng tin cậy, cài đặt phần mềm phòng chống mã độc; thiết lập chế độ tự động cập nhật phần mềm phòng chống mã độc, chế độ tự động rà quét mã độc khi sao chép, mở các tập tin, chế độ rà quét máy tính định kỳ hằng tuần.

2. Khuyến khích cơ quan đầu tư, mua sắm thiết bị công nghệ thông tin sản xuất trong nước. Nếu mua sắm thiết bị công nghệ thông tin nhập khẩu thuộc danh mục sản phẩm, hàng hóa có khả năng gây mất an toàn thuộc trách nhiệm quản lý của Bộ Thông tin và Truyền thông quy định.

3. Kết nối máy tính/thiết bị đầu cuối của người sử dụng vào hệ thống

a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin và các quy định của cơ quan, tổ chức;

b) Khi cài đặt, kết nối máy tính/thiết bị đầu cuối phải thực hiện theo hướng dẫn/quy trình dưới sự giám sát của bộ phận chuyên trách về an toàn thông tin;

c) Đối với hệ thống thông tin có cấp độ 3 trở lên, máy tính/thiết bị đầu cuối phải được xử lý điểm yếu an toàn thông tin, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống.

4. Trong quá trình sử dụng thiết bị đầu cuối

a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ 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 để kịp thời ngăn chặn và xử lý.

Điều 14. Quản lý giám sát an toàn hệ thống thông tin

1. Sở Ngoại vụ phải triển khai hệ thống giám sát an toàn thông tin đáp ứng các yêu cầu tại Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin.

3. Đối với các hệ thống thông tin, phần mềm, ứng dụng, cơ sở dữ liệu không được đặt tại Trung tâm tích hợp dữ liệu tỉnh thì Sở Ngoại vụ có trách nhiệm tự thực hiện hoặc yêu cầu doanh nghiệp cung cấp dịch vụ bảo đảm các yêu cầu giám sát an toàn hệ thống thông tin theo quy định của pháp luật.

4. Định kỳ hàng năm tổ chức đánh giá, kiểm tra đối với hệ thống thông tin nội bộ tại cơ quan. Thực hiện các biện pháp bảo trì cần thiết để bảo đảm khả năng xử lý và tính sẵn sàng của hệ thống thông tin.

Điều 15. 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 cán bộ quản trị hệ thống;

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. Phân nhóm sự cố an toàn thông tin

a) Sự cố do bị tấn công mạng: tấn công từ chối dịch vụ; tấn công giả mạo; tấn công sử dụng mã độc; truy cập trái phép, chiếm quyền điều khiển; tấn công thay đổi giao diện; tấn công mã hóa phần mềm, dữ liệu, thiết bị; phá hoại thông tin, dữ liệu, phần mềm; nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu; các hình thức tấn công mạng khác.

b) Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật;

c) Sự cố do lỗi của người quản trị, vận hành hệ thống;

d) Sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn. Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin: Hoạt động ứng cứu sự cố an toàn thông tin mạng huy động các ngu n lực nằm ngoài phạm vi của đơn vị vận hành hệ thống thông tin để đối phó với các sự cố quy định tại khoản 1 điều này.

3. Phân loại mức độ nghiêm trọng sự cố

a) Thấp: Sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan;

b) Trung bình: Sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của cơ quan;

c) Cao: Sự cố tác động đến khả năng vận hành của hệ thống thông tin, ảnh hưởng đến dữ liệu, thiết bị, gây ảnh hưởng đến hoạt động chung của cơ quan, đơn vị và hoạt động cung cấp dịch vụ công cho người dân, doanh nghiệp;

d) Nghiêm trọng: sự cố gây gián đoạn hoặc đình trệ hệ thống trong một khoảng thời gian ngắn, ảnh hưởng nghiêm trọng đến dữ liệu, thiết bị của hệ thống, gây thiệt hại nghiêm trọng cho cơ quan, đơn vị và người dân, doanh nghiệp;

đ) Đặc biệt nghiêm trọng: Sự cố làm tê liệt toàn bộ hoạt động của hệ thống, gây thiệt hại đặc biệt nghiêm trọng cho cơ quan, đơn vị và người dân, doanh nghiệp, đe dọa trật tự an toàn xã hội.

4. 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 Sở Ngoại vụ 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 theo quy chế nội bộ của cơ quan. 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;

(Xử lý khẩn cấp: Khi phát hiện hệ thống bị tấn công, thông qua các dấu hiệu như luồng, tin (traffic) tăng lên bất ngờ, nội dung trang chủ bị thay đổi, hệ thống hoạt động rất chậm khác thường,... cần thực hiện các bước cơ bản sau: Ngắt kết nối máy chủ ra khỏi mạng. Sao chép logfile và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ (phục vụ cho công tác phân tích); Khôi phục hệ thống bằng cách chuyển dữ liệu backup mới nhất để hệ thống hoạt động.)

c) Bước 3: Báo sự cố đến Sở Thông tin và Truyền thông theo mẫu số 01 kèm theo Quy chế;

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: Cán bộ chuyên trách CNTT của Sở lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố theo mẫu số 02 kèm theo Quy chế này. Lãnh đạo cơ quan phải chỉ đạo kịp thời để khắc phục và hạn chế thiệt hại, báo cáo bằng văn bản cho Sở Thông tin và Truyền thông.

5. Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của cơ quan; cán bộ chuyên trách CNTT của Sở phải báo cáo ngay cho Lãnh đạo cơ quan và thông tin đến Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ.

6. Cán bộ 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, 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 III

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

Điều 16. Trách nhiệm của Sở Ngoại vụ

1. Thủ trưởng cơ quan có trách nhiệm tổ chức phổ biến các quy định tại Quy chế này và chịu trách nhiệm trong công tác bảo đảm an toàn thông tin mạng của đơn vị mình.

2. Thực hiện xác định cấp độ an toàn thông tin và bảo đảm an toàn cho hệ thống thông tin của đơn vị quản lý theo quy định tại Luật An toàn thông tin mạng và các văn bản hướng dẫn thi hành Luật An toàn thông tin mạng.

3. Phân công cán bộ chuyên trách bảo đảm an toàn thông tin của cơ quan; chỉ đạo công chức và người lao động nghiêm túc chấp hành các quy định về bảo đảm an toàn thông tin; tạo điều kiện để cán bộ phụ trách an toàn 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; xác định các yêu cầu, trách nhiệm bảo đảm an toàn thông tin đối với công chức thuộc Sở.

4. Ban hành quy trình nội bộ về bảo đảm an toàn thông tin gồm các nội dung cơ bản như quy định về quản lý hạ tầng mạng, bảo đảm an toàn dữ liệu, bảo đảm an toàn thiết bị và người dùng đầu cuối phù hợp với Quy chế của tỉnh và các quy định của pháp luật.

5. 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.

6. 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.

7. Hàng năm bố trí kinh phí cho việc ứng dụng công nghệ thông tin nói chung và công tác bảo đảm an toàn thông tin mạng nói riêng trong nội bộ cơ quan; 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.

8. Cử đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin. Phân công lãnh đạo phụ trách công tác đảm bảo an toàn thông tin đối với các hệ thống thông tin và cơ sở dữ liệu do đơn vị quản lý.

9. Thực hiện các báo cáo về an toàn thông tin mạng khi được Sở Thông tin và Truyền thông yêu cầu.

Điều 17. Trách nhiệm của công chức và người lao động thuộc Sở

1. Trách nhiệm của cán bộ phụ trách về an toàn thông tin/công nghệ thông tin của Sở

a) Chịu trách nhiệm bảo đảm an toàn thông tin mạng của cơ quan;

b) Tham mưu lãnh đạo Sở ban hành các quy chế, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin mạng;

c) Thực hiện việc giám sát, đánh giá, báo cáo lãnh đạo Sở các rủi ro mất an toàn thông tin mạng và mức độ nghiêm trọng của các rủi ro đó;

d) Phối hợp với các đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn thông tin mạng;

đ) 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 các quy chế, quy trình nội bộ 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. Thường xuyên cập nhật những chính sách, thủ tục an toàn thông tin của đơn vị cũng như thực hiện những hướng dẫn về an toàn, an ninh thông tin của cán bộ phụ trách CNTT của Sở như một phần của công việc;

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

c) Hạn chế việc sử dụng chức năng chia sẻ tài nguyên (sharing), khi sử dụng chức năng này cần bật thuộc tính bảo mật bằng mật khẩu và thực hiện việc thu hồi chức năng này khi đã sử dụng xong. Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và cán bộ phụ trách công nghệ thông tin của Sở, để kịp thời ngăn chặn và xử lý;

d) Các máy tính khi không sử dụng trong thời gian dài (quá 2 giờ làm việc) cần tắt máy hoặc ngưng kết nối mạng, để tránh bị các hacker lợi dụng, sử dụng chức năng điều khiển từ xa dùng máy tính của mình tấn công vào các hệ thống thông tin khác.

đ) Sử dụng chức năng mã hóa ở mức hệ điều hành bảo đảm các dữ liệu nhạy cảm như tài khoản, mật khẩu, các tập tin văn bản,... được mã hóa trước khi truyền trên môi trường mạng. Các tập tin gửi đính kèm bởi thư điện tử hoặc được tải xuống từ Internet hay các thiết bị lưu trữ gắn vào hệ thống cần được kiểm tra để phòng chống lây nhiễm virus hoặc phần mềm gián điệp gây mất mát thông tin.

e) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được cơ quan hoặc đơn vị chuyên môn tổ chức.

Điều 18. Tổ chức thực hiện

1. Căn cứ Quy chế này, lãnh đạo các đơn vị thuộc Sở có trách nhiệm tổ chức triển khai thực hiện Quy chế này trong phạm vi quản lý của mình.

2. Cán bộ phụ trách về an toàn thông tin/công nghệ thông tin của Sở có trách nhiệm theo dõi, đôn đốc, kiểm tra, đánh giá việc thực hiện Quy chế, báo cáo theo định kỳ hằng năm hoặc đột xuất theo yêu cầu của Sở Thông tin và Truyền thông.

3. Các phòng, đơn vị, công chức và người lao động thuộc Sở có hành vi vi phạm quy chế này thì tùy theo tính chất, mức độ vi phạm 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.

4. Trong quá trình thực hiện quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời về Văn phòng Sở để tổng hợp, báo cáo Giám đốc Sở xem xét điều chỉnh, bổ sung./.