UBND TỈNH BÌNH ĐỊNH
SỞ NGOẠI VỤ

TÀI LIỆU THUYẾT MINH HỒ SƠ ĐỀ XUẤT CẤP ĐỘ ĐỐI VỚI HỆ THỐNG THÔNG TIN CỦA SỞ NGOẠI VỤ

Bình Định, tháng 5/2024

MỤC LỤC

PHẦN I

THUYẾT MINH TỔNG QUAN VỀ HỆ THỐNG THÔNG TIN

1. Khái niệm hệ thống thông tin

- Hệ thống thông tin được hiểu là tập hợp bao gồm hạ tầng phần cứng và phần mềm được kết nối với nhau thông qua các chuẩn, các giao thức và kết nối vật lý nhằm đảm bảo phân tích và cung cấp thông tin cho người dùng.

- Mỗi hệ thống thông tin có quy mô và phạm vi hoạt động khác nhau. Tùy theo mục đích sử dụng và tính chất công việc mà các hệ thống được thiết kế ở các cấp độ khác nhau cho phù hợp.

- Ngoài tính chất hoạt động độc lập, các hệ thống thông tin khác nhau cũng có thể chia sẻ dữ liệu hoặc cùng thực hiện một số nhiệm vụ chung.

2. Thông tin Chủ quản hệ thống thông tin

- Tên Tổ chức: Uỷ ban nhân dân tỉnh Bình Định

- Người đại diện: **Phạm Anh Tuấn**

- Chức vụ: Chủ tịch Uỷ ban nhân dân tỉnh.

- Địa chỉ: 01A Trần Phú, TP. Quy Nhơn, tỉnh Bình Định

- Điện thoại: 02563.822294.

3. Thông tin Đơn vị vận hành

Tên Đơn vị vận hành: Sở Ngoại vụ tỉnh Bình Định

- Số Quyết định thành lập: 195/QĐ-UBND ngày 18/4/2012

- Người đại diện: **Nguyễn Thái Bình**

- Chức vụ: Giám đốc Sở

- Địa chỉ: 59-61 Lê Hồng Phong, TP. Quy Nhơn, tỉnh Bình Định

- Thông tin liên hệ: Số điện thoại: 0256.3820202

Email: vp@songoaivu.binhdinh.gov.vn

4. Mô tả phạm vi, quy mô của hệ thống

- Phạm vi, quy mô của hệ thống: Hệ thống thông tin Sở Ngoại vụ được thiết lập để phục vụ công tác chỉ đạo điều hành, cung cấp thông tin và cung cấp dịch vụ công trực tuyến của Sở Ngoại vụ.

- Đối tượng phục vụ của hệ thống:

+ Toàn thể công chức và người lao động của Sở;

+ Các tổ chức, doanh nghiệp, người dân muốn khai thác thông tin trên Trang thông tin điện tử của Sở.

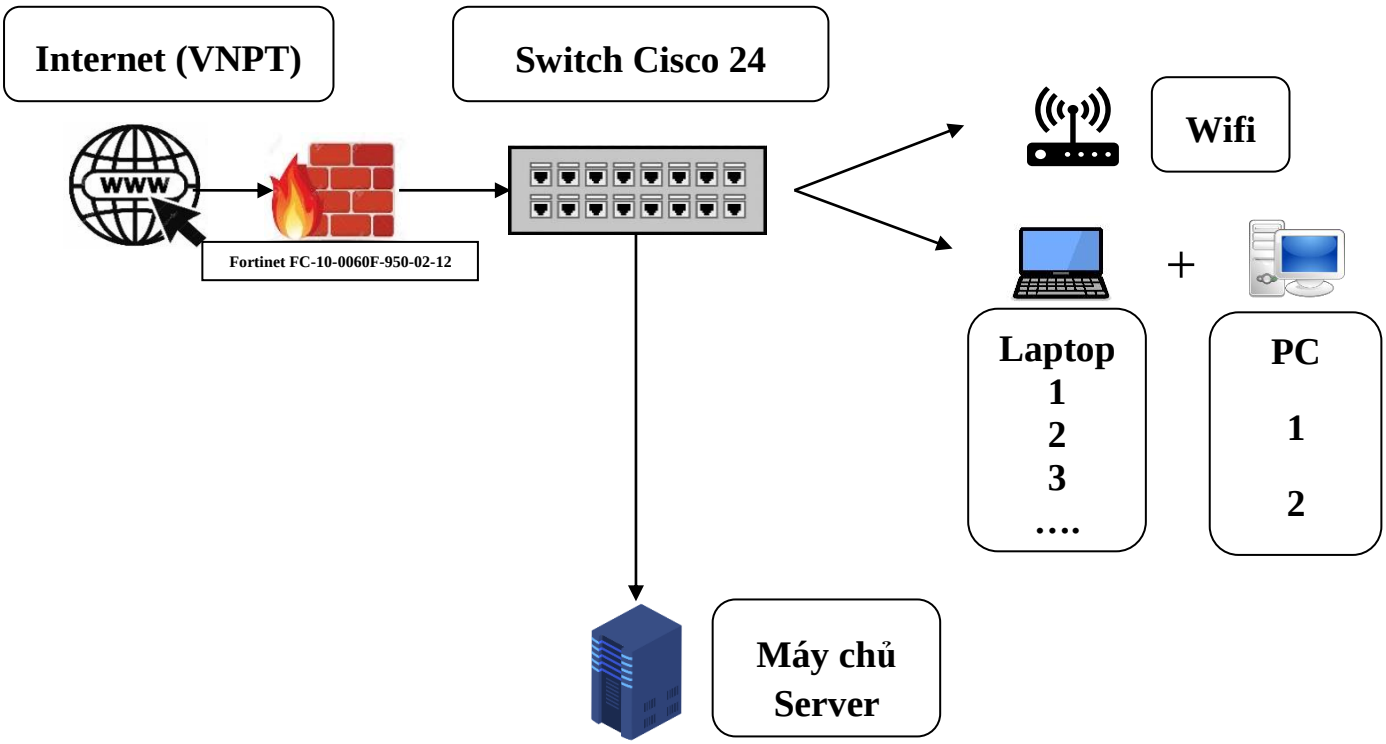
- Danh mục các hệ thống thông tin thành phần/các dịch vụ được cung cấp bởi hệ thống Sở Ngoại vụ:

+ Hệ thống Trang thông tin điện tử.

+ Hệ thống mạng nội bộ - LAN của cơ quan.

5. Mô tả cấu trúc của hệ thống

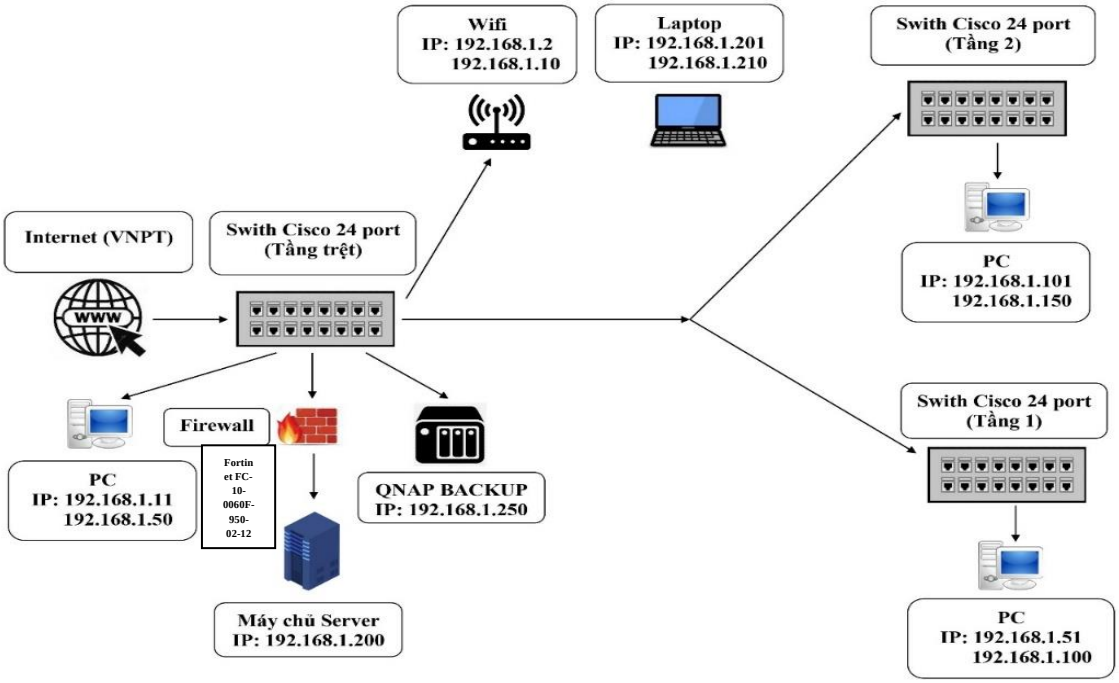
a) Sơ đồ logic tổng thể



Hình 1: Sơ đồ logic tổng thể hệ thống mạng

Các kết nối của thiết bị cùng chung một vùng mạng LAN. Kết nối của các PC và Server trực tiếp đến Switch, kết nối của Switch trực tiếp đến thiết bị Router. Thiết bị Router kết nối đến nhà cung cấp dịch vụ Internet (VNPT).

b) Sơ đồ kết nối vật lý



Hình 2: Sơ đồ kết nối vật lý tổng thể hệ thống mạng

c) Danh mục thiết bị sử dụng trong hệ thống

STT	Tên thiết bị/Chủng loại	Vị trí triển khai	Mục đích sử dụng
1	Router Draytek (Vigor 2912F)	Văn phòng Sở (tầng trệt)	Kết nối đến Internet; và định tuyến động với các Router của 02 ISP.
2	Switch 24 port TP-Link	Đặt tại các đầu mối các tầng	Bộ chia kết nối có dây, truyền tín hiệu đến các thiết bị khác.
3	Switch 8 port TP-Link Switch 5 port TP-Link Igate	Đặt tại các Phòng thuộc Sở, phòng họp, hội trường	Bộ chia kết nối có dây, truyền tín hiệu đến các thiết bị khác.
4	Wireless Access point	Tầng trệt: 02 Tầng 1: 03 Tầng 2: 02	Nhận tín hiệu dây từ Router, phát không dây tín hiệu Internet cho các thiết bị dùng wireless.
5	Firewall Fortinet FC-10-0060F-950-02-12	Văn phòng Sở (triển khai tháng 9/2022)	Ngăn chặn những truy cập trái phép xâm phạm vào máy tính hoặc hệ thống mạng.

d) Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống

STT	Tên dịch vụ	Máy chủ triển khai	Mục đích sử dụng
1	Trang thông tin điện tử của Sở Ngoại vụ	Hosting tại máy chủ của cơ quan/	Cung cấp tin tức và các dịch vụ giải quyết TTHC bên trong hệ thống và cung cấp thông tin công khai về DVCTT, tình trạng giải quyết TTHC cho người sử dụng bên ngoài Internet…
2	Hệ thống mạng nội bộ- LAN của cơ quan	Mô hình Máy khách/ Máy chủ (Client/Server)	Các máy tính cá nhân được kết nối với nhau tạo nên mạng LAN để chia sẻ tài nguyên mạng, chia sẻ máy in mạng.
3	Hệ thống Camera an ninh cơ quan	Đầu thu – Camera vệ tinh	Hệ thống giám sát an ninh tại Sở Ngoại vụ.

PHẦN II
THUYẾT MINH ĐỀ XUẤT CẤP ĐỘ AN TOÀN HỆ THỐNG THÔNG TIN

1. Danh mục hệ thống thông tin và cấp độ đề xuất tương ứng

Căn cứ Điều 8 Nghị định số 85/2016/NĐ-CP ngày 01/7/2017 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ, Hệ thống thông tin của Sở Ngoại vụ là hệ thống cơ sở hạ tầng thông tin thuê dịch vụ và hệ thống mạng nội bộ.

STT	Hệ thống	Loại thông tin xử lý	Loại hình HTTT	Cấp độ đề xuất	Căn cứ đề xuất
1	Trang thông tin điện tử của Sở Ngoại vụ	Trang riêng	Hệ thống thông tin phục vụ hoạt động nội bộ trong phạm vi Sở; hoặc người dân, doanh nghiệp quan tâm đến thông tin đăng trên web của Sở và TTHC do Sở cung cấp.	Theo cấp độ của Trung tâm CNTT và Truyền thông	Theo Quyết định số 2634/QĐ-UBND ngày 02/7/2020 của UBND tỉnh phê duyệt cấp độ an toàn hệ thống thông tin
2	Hệ thống mạng nội bộ - LAN của cơ quan	Thông tin nội bộ cơ quan	Hệ thống cơ sở hạ tầng thông tin phục vụ hoạt động của cơ quan.	2	Khoản 3, Điều 8 Nghị định số 85/2016/NĐ-CP
3	Hệ thống Camera an ninh cơ quan	Đầu thu – Camera vệ tinh	Hệ thống giám sát an ninh tại Sở Ngoại vụ.	2	Điều 8 Nghị định số 85/2016/NĐ-CP

2. Thuyết minh chi tiết đối với hệ thống thông tin

- Trang thông tin điện tử: Cung cấp thông tin hoạt động chuyên ngành của Sở đến với người dân, tổ chức, doanh nghiệp; Cung cấp các dịch vụ hành chính công; Cung cấp thông tin chỉ đạo điều hành của lãnh đạo Sở; văn bản pháp luật.

- Hệ thống mạng nội bộ (LAN) của cơ quan: Hệ thống phần cứng và cáp kết nối đảm bảo truyền tải thông tin giữa các hệ thống và thiết bị bên trong và bên ngoài mạng LAN. Sở Ngoại vụ tiến hành xây dựng phương án đảm bảo an toàn hệ thống thông tin đối với hệ thống này *như phần III*.

- Hệ thống Camera an ninh cơ quan: Hệ thống trang bị chức năng ghi hình, theo dõi, giám sát mọi hoạt động tại cơ quan.

PHẦN III
THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN

I. Thuyết minh phương án bảo đảm an toàn thông tin về quản lý với cấp độ 2

1. Thiết lập chính sách an toàn thông tin

1.1. Chính sách an toàn thông tin

	Xây dựng chính sách an toàn thông tin
Hiện trạng	Đáp ứng tại các Điều 11, 13, 14 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.
Phương án	**Điều 11. 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 13. Bảo đảm an toàn dữ liệu** 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). 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 14. Bảo đảm an toàn thiết bị đầu cuối** 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.

1.2. Xây dựng và công bố

Yêu cầu	Quy định về xây dựng và công bố Quy chế bảo đảm an toàn thông tin
Hiện trạng	Đáp ứng
Phương án	**Điều 20. Xây dựng, rà soát, cập nhật, bổ sung Quy chế** Định kỳ 02 năm hoặc khi có thay đổi chính sách an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung Quy chế bảo đảm an toàn thông tin.

	Tham chiếu Điều 20 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.

1.3. Rà soát, sửa đổi

Yêu cầu	Có quy định về việc rà soát, sửa đổi Quy chế bảo đảm an toàn thông tin
Hiện trạng	Đáp ứng
Phương án	**Điều 20. Xây dựng, rà soát, cập nhật, bổ sung Quy chế** Định kỳ 02 năm hoặc khi có thay đổi chính sách an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung Quy chế bảo đảm an toàn thông tin. Trong quá trình thực hiện, nếu có những 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. *Tham chiếu Điều 20 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

2. Tổ chức bảo đảm an toàn thông tin

2.1. Đơn vị chuyên trách về an toàn thông tin

Yêu cầu	Nhân sự chuyên trách về an toàn thông tin
Hiện trạng	Đáp ứng
Phương án	**Điều 16. Ứng cứu sự cố an toàn thông tin** 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. **Điều 17. 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. 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 18. 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. *Tham chiếu Điều 16, 17, 18 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

2.2. Phối hợp với những cơ quan/tổ chức có thẩm quyền

Yêu cầu	Có quy định phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin
Hiện trạng	Đáp ứng
Phương án	**Điều 16. Ứng cứu sự cố an toàn thông tin** 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 về Sở 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 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 được quy định tại Quyết định số 22/2021/QĐ-UBND ngày 11/6/2021 của UBND tỉnh Bình Định. *Tham chiếu điểm 4, Điều 16 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

3. Bảo đảm nguồn nhân lực

3.1. Tuyển dụng

Yêu cầu	Có quy định về tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ
Hiện trạng	Đáp ứng
Phương án	**Điều 10. 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. *Tham chiếu Điều 10 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

3.2. Trong quá trình làm việc

a. Có quy định về việc thực hiện nội quy, quy chế bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống

Yêu cầu	Có quy định về việc thực hiện nội quy, quy chế bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống
Hiện trạng	Đáp ứng
Phương án	**Điều 17. 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. 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 18. 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. *Tham chiếu Điều 17, 18 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

b. Có kế hoạch và định kỳ hàng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng

Yêu cầu	Có kế hoạch và định kỳ hàng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng
Hiện trạng	Đáp ứng
Phương án	**Điều 17. 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. 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. *Tham chiếu Điều 17 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

c. Chấm dứt hoặc thay đổi công việc

Yêu cầu	Có quy định đối với cán bộ nghỉ hoặc thay đổi công việc
Hiện trạng	Đáp ứng
Phương án	**Điều 9. Quy định về cấp phát, thu hồi, cập nhật và quản lý các tài khoản truy cập vào hệ thống thông tin** 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. *Tham chiếu khoản 2, Điều 9 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

Yêu cầu	Có quy trình và thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.
Hiện trạng	Đáp ứng
Phương án	**Điều 13. Bảo đảm an toàn dữ liệu** 1. Quản lý tài khoản và chữ ký số 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. *Tham chiếu điểm e, khoản 1, Điều 13 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

4. Quản lý thiết kế, xây dựng hệ thống thông tin

4.1. Thiết kế an toàn hệ thống thông tin

a. Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin

Yêu cầu	Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin
Hiện trạng	Đáp ứng
Phương án	**Điều 6. 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 Ngoại vụ 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 trước khi 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. *Tham chiếu Điều 6 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

b. Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin

Yêu cầu	Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin
Hiện trạng	Đáp ứng
Phương án	Tham chiếu Điều 6 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.

c. Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ

Yêu cầu	Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ
Hiện trạng	Đáp ứng
Phương án	Tham chiếu Điều 6 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.

d. Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin

Yêu cầu	Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin
Hiện trạng	Đáp ứng
Phương án	Tham chiếu Điều 6 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.

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

Yêu cầu	Có quy định khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống
Hiện trạng	Đáp ứng
Phương án	**Điều 20. Xây dựng, rà soát, cập nhật, bổ sung Quy chế** Định kỳ 02 năm hoặc khi có thay đổi chính sách an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung Quy chế bảo đảm an toàn thông tin. *Tham chiếu Điều 20 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

4.2. Phát triển phần mềm thuê khoán

a. Có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán

Yêu cầu	Có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán
Hiện trạng	Đáp ứng
Phương án	**Điều 7. 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. *Tham chiếu Điều 7 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

b. Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm

Yêu cầu	Có quy định yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm
Hiện trạng	Đáp ứng
Phương án	**Điều 6. 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 Ngoại vụ 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 trước khi 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. *Tham chiếu Điều 6 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

4.3. Thử nghiệm và nghiệm thu hệ thống

a. Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng

Yêu cầu	Có quy định về việc thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng
Hiện trạng	Đáp ứng
Phương án	**Điều 6. Yêu cầu thiết kế, xây dựng hệ thống thông tin** 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.

	Tham chiếu khoản 3, Điều 6 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.

b. Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống

Yêu cầu	Có yêu cầu về nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống
Hiện trạng	Đáp ứng
Phương án	Quy định đối với việc thử nghiệm và nghiệm thu hệ thống: Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống. *Tham chiếu Điều 6 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

c. Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống

Yêu cầu	Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống
Hiện trạng	Đáp ứng
Phương án	Quy định đối với việc thử nghiệm và nghiệm thu hệ thống: Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống. **Điều 6. Yêu cầu thiết kế, xây dựng hệ thống thông tin** 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. *Tham chiếu khoản 3, Điều 6 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

5. Quản lý vận hành hệ thống thông tin

5.1. Quản lý an toàn mạng

a. Quản lý, vận hành hoạt động bình thường của hệ thống

Yêu cầu	Có quy định về quản lý, vận hành hoạt động bình thường của hệ thống
Hiện trạng	Đáp ứng
Phương án	**Điều 11. 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. *Tham chiếu Điều 11 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

b. Cập nhật; sao lưu dự phòng các tập tin cấu hình hệ thống và khôi phục hệ thống sau khi xảy ra sự cố

Yêu cầu	Có quy định về cập nhật; sao lưu dự phòng các tập tin cấu hình hệ thống và khôi phục hệ thống sau khi xảy ra sự cố
Hiện trạng	Đáp ứng
Phương án	**Điều 13. 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. *Tham chiếu Điều 13 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

c. Truy cập và quản lý cấu hình hệ thống

Yêu cầu	Truy cập và quản lý cấu hình hệ thống
Hiện trạng	Đáp ứng
Phương án	**Điều 13. 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. *Tham chiếu khoản 1, Điều 13 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

5.2. Quản lý an toàn máy chủ và ứng dụng

a. Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ

Yêu cầu	Có quy định về quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ
Hiện trạng	Đáp ứng
Phương án	**Điều 12. 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 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). *Tham chiếu Điều 12 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

b. Truy cập mạng của máy chủ

Yêu cầu	Có quy định quản lý truy cập mạng của máy chủ
Hiện trạng	Đáp ứng
Phương án	**Điều 12. 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 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 15. 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. 2. 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. 3. 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. *Tham chiếu Điều 12,15 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

c. Truy cập và quản trị máy chủ và ứng dụng

Yêu cầu	Có quy định quản lý truy cập và quản trị máy chủ và ứng dụng
Hiện trạng	Đáp ứng
Phương án	**Điều 12. 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. 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). *Tham chiếu khoản 1 và khoản 5 Điều 12 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

d. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố

Yêu cầu	Có quy định về cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố
Hiện trạng	Đáp ứng
Phương án	**Điều 13. Bảo đảm an toàn dữ liệu** 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).

	Tham chiếu khoản 2,3,4,5,6 Điều 13 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.

5.3. Quản lý an toàn dữ liệu

a. Chính sách, quy trình dự phòng và khôi phục dữ liệu

Yêu cầu	Có chính sách, quy trình dự phòng và khôi phục dữ liệu
Hiện trạng	Đáp ứng
Phương án	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. *Tham chiếu điểm 4, Điều 13 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

b. Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ

Yêu cầu	Có quy định định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ
Hiện trạng	Đáp ứng một phần
Phương án	**Điều 13. Bảo đảm an toàn dữ liệu** 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). **Điều 15. 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. 2. 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. 3. 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. *Tham chiếu khoản 4,5,6 Điều 13, 15 Quy chế bảo đảm an*

	toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.

5.4. Quản lý sự cố an toàn thông tin

a. Phân nhóm sự cố an toàn thông tin mạng

Yêu cầu	Có quy định về phân nhóm sự cố an toàn thông tin mạng
Hiện trạng	Đáp ứng
Phương án	**Điều 16. Ứng cứu sự cố an toàn thông tin** 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. *Tham chiếu khoản 2, Điều 16 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

b. Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng

Yêu cầu	Có phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng
Hiện trạng	Đáp ứng
Phương án	**Điều 16. Ứng cứu sự cố an toàn thông tin** 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. *Tham chiếu khoản 6 Điều 16 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

c. Kế hoạch ứng phó sự cố an toàn thông tin mạng

Yêu cầu	Xây dựng kế hoạch ứng phó sự cố an toàn thông tin mạng
Hiện trạng	Đáp ứng
Phương án	Tham chiếu Điều 16 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.

d. Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin

Yêu cầu	Có quy định về quản lý giám sát, phát hiện và cảnh báo sự cố an toàn thông tin
Hiện trạng	Đáp ứng
Phương án	**Điều 15. 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. 2. 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. 3. 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. *Tham chiếu Điều 15 Quy chế bảo đảm an toàn thông tin theo*

	Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.

đ. Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường

Yêu cầu	Có quy trình ứng cứu sự cố an toàn thông tin mạng thông thường
Hiện trạng	Đáp ứng
Phương án	**Điều 16. Ứng cứu sự cố an toàn thông tin** 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. *Tham chiếu khoản 2 Điều 16 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

e. Quy trình ứng cứu sự cố an toàn thông tin mạng nghiêm trọng

Yêu cầu	Có quy trình ứng cứu sự cố an toàn thông tin mạng nghiêm trọng
Hiện trạng	Đáp ứng
Phương án	**Điều 16. Ứng cứu sự cố an toàn thông tin** 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. 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. *Tham chiếu khoản 3,5 Điều 16 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

g. Cơ chế 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	Có quy định về cơ chế 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
Hiện trạng	Đáp ứng
Phương án	**Điều 16. Ứng cứu sự cố an toàn thông tin** 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 về Sở 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 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 được quy định tại Quyết định số 22/2021/QĐ-UBND ngày 11/6/2021 của UBND tỉnh Bình Định. *Tham chiếu khoản 4 Điều 16 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

5.5. Quản lý an toàn người sử dụng đầu cuối

a. Quản lý truy cập, sử dụng tài nguyên nội bộ

Yêu cầu	Có quy định về quản lý truy cập, sử dụng tài nguyên nội bộ
Hiện trạng	Đáp ứng
Phương án	**Điều 14. 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. *Tham chiếu Điều 14 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

b. Quản lý truy cập mạng và tài nguyên trên Internet

Yêu cầu	Có quy định về quản lý truy cập mạng và tài nguyên trên Internet
Hiện trạng	Đáp ứng
Phương án	**Điều 9. 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 !, @, #, $, %,...). *Tham chiếu khoản 1,2,3 Điều 9 Quy chế bảo đảm an toàn thông tin theo Quyết định số 1368/QĐ-SNgV ngày 04/12/2023.*

5.6. Phương án Quản lý rủi ro an toàn thông tin

Yêu cầu	Có chính sách, quy trình quản lý quản lý rủi ro an toàn thông tin
Hiện trạng	Đáp ứng. Quy chế đã đưa ra quy định về chính sách, đã **đáp ứng** yêu cầu một phần về quy trình Kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin sẽ bổ sung trong vòng 06 tháng khi hồ sơ đề xuất cấp độ được phê duyệt.
Phương án	Phương án quản lý rủi ro an toàn thông tin được xây dựng trong Quy chế bảo đảm an toàn, đã làm rõ các nội dung. 1. Xác định mức rủi ro. 2. Quy trình đánh giá và quản lý rủi ro. 3. Biện pháp kiểm soát rủi ro.

5.7. Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin

Yêu cầu	Có quy định, quy trình về Kết thúc vận hành, khai thác, thanh lý, hủy bỏ
Hiện trạng	Đáp ứng
Phương án	Kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống a) Cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác. b) Trước khi gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống: Phải sao lưu dữ liệu trước khi gỡ bỏ. Phải xoá dữ liệu, ghi đè dữ liệu, format ổ cứng trên thiết bị. Một số trường hợp đặc biệt có thể cần phải phá huỷ vật lý thiết bị/vật lưu trữ trước khi bỏ đi.

II. Thuyết minh phương án kỹ thuật đối với Hệ thống thành phần cấp độ

Hệ thống thông tin: Hệ thống mạng nội bộ (LAN) của Sở Ngoại vụ được đề xuất là cấp độ 2. Do đó, các thiết bị được sử dụng để triển khai hệ thống và các thành phần khác trong hệ thống như hạ tầng mạng, hệ thống lưu trữ… được thuyết minh phương án đáp ứng yêu cầu cấp độ 2 như sau:

1. Bảo đảm an toàn mạng

1.1. Kiểm soát truy cập từ bên ngoài mạng

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet.	Có	Hệ thống sử dụng tường lửa tích hợp trong thiết bị Modem/Router ngăn chặn tất cả truy cập từ mạng Internet vào vùng mạng nội bộ và vùng mạng wifi công cộng.
2	Kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả truy cập tới các dịch vụ, ứng dụng mà hệ thống không cung cấp hoặc không cho phép truy cập từ bên ngoài.	Có	Hệ thống sử dụng tường lửa tích hợp trong thiết bị Modem/Router ngăn chặn tất cả truy cập từ mạng Internet vào vùng mạng nội bộ và vùng mạng wifi công cộng.

3	Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng.	Có	Hệ thống sử dụng tường lửa tích hợp trong thiết bị Modem/Router ngăn chặn tất cả truy cập từ mạng Internet vào vùng mạng nội bộ và vùng mạng wifi công cộng.

1.2. Nhật ký hệ thống

Yêu cầu **Thiết bị**	Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị hệ thống.	Sử dụng máy chủ thời gian trong hệ thống để đồng bộ thời gian.
Modem/Router DrayTek Vigor 2915	Ghi nhật ký theo mặc định của thiết bị.	Đồng bộ thời gian theo thiết lập mặc định của thiết bị.
Fortinet FortiGate 60F	Ghi nhật ký theo mặc định của thiết bị.	Đồng bộ thời gian theo thiết lập mặc định của thiết bị.
Hệ thống máy trạm (máy tính cá nhân)	Ghi nhật ký theo mặc định của hệ điều hành.	Đồng bộ thời gian theo thiết lập mặc định của hệ điều hành.

1.3. Phòng chống xâm nhập

STT	**Yêu cầu**	**P/A**	**Ghi chú/Mô tả**
1	Có phương án phòng chống xâm nhập để bảo vệ các vùng mạng trong hệ thống.	Đáp ứng	Hệ thống sử dụng tường lửa tích hợp trong thiết bị Modem/Router ngăn chặn tất cả truy cập từ mạng Internet vào vùng mạng nội bộ và vùng mạng wifi công cộng.
2	Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng.	Đáp ứng	Hệ thống sử dụng tường lửa tích hợp trong thiết bị Modem/Router ngăn chặn tất cả truy cập từ mạng Internet vào vùng mạng nội bộ và vùng mạng wifi công cộng.

1.4. Bảo vệ thiết bị hệ thống

Yêu cầu **Thiết bị**	Cấu hình chức năng xác thực trên các thiết bị.	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị thiết bị từ xa.	Hạn chế các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa.
Modem/Router DrayTek Vigor 2915	Xác thực bằng usename / password	Chỉ cho phép máy tính quản trị trong mạng nội bộ.	Chỉ cho phép IP của máy tính quản trị trong mạng nội bộ.
Fortinet FortiGate 60F	Xác thực bằng usename / password	Chỉ cho phép máy tính quản trị trong mạng nội bộ.	Chỉ cho phép IP của máy tính quản trị trong mạng nội bộ.
Hệ thống máy trạm (máy tính cá nhân)	Xác thực bằng usename / password của hệ điều hành	Không cho phép truy cập từ xa.	Không cho phép truy cập từ xa.

2. Bảo đảm an toàn máy chủ

Có thiết lập yêu cầu bảo đảm mật khẩu trên ứng dụng đủ độ phức tạp (chữ hoa, chữ thường, số và ký tự đặc biệt) để hạn chế tấn công dò quét mật khẩu; các thông tin xác thực phải được lưu trữ dưới dạng mã hóa.

Sử dụng kết nối mạng mã hóa trong việc quản trị từ xa: Mã hóa thông tin, dữ liệu trước khi truyền dữ liệu đi để đảm bảo không bị lộ thông tin, dữ liệu trên đường truyền.

2.1. Xác thực

Yêu cầu **Ứng dụng**	Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng.	Lưu trữ có mã hóa thông tin xác thực hệ thống.	Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng.	Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định.
Hệ thống máy trạm (máy tính cá nhân)	Xác thực bằng usename / password của hệ điều hành	+	+	+
Kết nối mạng wifi	Xác thực bằng usename / password	+	+	+

2.2. Kiểm soát truy cập

Yêu cầu	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa.	Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng.	Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa.
Ứng dụng			
Hệ thống máy trạm (máy tính cá nhân)	Không cho phép	Thiết lập thời gian chờ để khoá màn hình	Không cho phép

2.3. Nhật ký hệ thống

Yêu cầu	Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau: (1) Thông tin truy cập ứng dụng (2) Thông tin đăng nhập khi quản trị ứng dụng; (3) Thông tin các lỗi phát sinh trong quá trình hoạt động; (4) Thông tin thay đổi cấu hình ứng dụng.	Nhật ký hệ thống phải được lưu trữ trong khoảng thời gian tối thiểu là 01 tháng
Ứng dụng		
Hệ thống máy trạm (máy tính cá nhân)	Ghi nhật ký theo mặc định của hệ điều hành	

2.4. Phòng chống xâm nhập

STT	Yêu cầu	P/A	Mô tả	Ghi chú
1	Có phương án phòng chống xâm nhập để bảo vệ các vùng mạng trong hệ thống	Đáp ứng	Sử dụng Firewall có chức năng ngăn chặn những truy cập trái phép xâm phạm vào máy tính hoặc hệ thống mạng	
2	Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng	Đáp ứng	Thực hiện định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng.	

2.5. Phòng chống phần mềm độc hại

Yêu cầu **Thiết bị**	Cấu hình chức năng xác thực trên các thiết bị	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị thiết bị từ xa	Hạn chế các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa
Modem/Router DrayTek Vigor 2915	Xác thực bằng usename / password	Chỉ cho phép máy tính quản trị trong mạng nội bộ	Chỉ cho phép IP của máy tính quản trị trong mạng nội bộ
Fortinet FortiGate 60F	Xác thực bằng usename / password	Chỉ cho phép máy tính quản trị trong mạng nội bộ	Chỉ cho phép IP của máy tính quản trị trong mạng nội bộ
Hệ thống máy trạm (máy tính cá nhân)	Xác thực bằng usename / password của hệ điều hành	Không cho phép truy cập từ xa	Không cho phép truy cập từ xa

3. Bảo đảm an toàn ứng dụng

3.1. Xác thực

Yêu cầu **Ứng dụng**	Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng	Lưu trữ có mã hóa thông tin xác thực hệ thống	Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng	Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định
Hệ thống máy trạm (máy tính cá nhân)	Xác thực bằng usename / password của hệ điều hành	+	+	+
Kết nối mạng wifi	Xác thực bằng usename / password	+	+	+

3.2. Kiểm soát truy cập

Yêu cầu	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa	Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng	Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa
Ứng dụng			
Hệ thống máy trạm (máy tính cá nhân)	Không cho phép	Thiết lập thời gian chờ để khoá màn hình	Không cho phép

3.3. Nhật ký hệ thống

Yêu cầu	Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau: (1) Thông tin truy cập ứng dụng (2) Thông tin đăng nhập khi quản trị ứng dụng; (3) Thông tin các lỗi phát sinh trong quá trình hoạt động (4) Thông tin thay đổi cấu hình ứng dụng.	Nhật ký hệ thống phải được lưu trữ trong khoảng thời gian tối thiểu là 01 tháng
Ứng dụng		
Hệ thống máy trạm (máy tính cá nhân)	Ghi nhật ký theo mặc định của hệ điều hành	

4. Bảo đảm an toàn dữ liệu

4.1. Bảo mật dữ liệu

Mã hóa các tập tin dữ liệu để bất kỳ ai cũng không thể đọc được ngoại trừ người nắm giữ khóa bí mật.

Công chức của Sở phải có trách nhiệm bảo mật dữ liệu nghiệp vụ trên máy tính của mình. Việc chia sẻ dữ liệu trên mạng phải đảm bảo an toàn, an ninh thông tin theo quy định và sử dụng các biện pháp rà quét các dữ liệu nhạy cảm khi truyền đi trên môi trường mạng.

Khi công chức chấm dứt hoặc thay đổi công việc, các tài khoản truy cập hệ thống, thông tin lưu trữ trên phương tiện lưu trữ sẽ được đóng và các thiết bị, máy móc, tài sản có liên quan được phân cho cán bộ, công chức khác tiếp quản.

Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản Bí mật Nhà nước, các phòng phải báo cáo cho người có thẩm quyền. Không được cho phép các công ty tư nhân hoặc người không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố; Lưu ý: máy tính dùng để soạn thảo văn bản Bí mật Nhà nước không được kết nối internet.

Trước khi thanh lý các máy tính trong các cơ quan nhà nước, cán bộ chuyên trách CNTT phải dùng các biện pháp kỹ thuật xoá bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

4.2. Sao lưu dự phòng

Sao lưu dữ liệu định kỳ, sử dụng mã Hash để mã hóa dữ liệu đã sao lưu và lưu trữ cùng dữ liệu được sao lưu. Sử dụng công cụ kiểm tra mã Hash để kiểm tra tính nguyên vẹn của dữ liệu bằng cách so sánh mã Hash nếu giống nhau thì dữ liệu sao lưu là nguyên vẹn (dữ liệu gốc) ngược lại dữ liệu sao lưu không còn nguyên vẹn.

Việc sao lưu được thực hiện định kỳ theo quy định của cơ quan.

Công chức phải có trách nhiệm tự sao lưu dữ liệu của cá nhân; quét và diệt virus trên máy tính cá nhân.

Phân loại cụ thể các dữ liệu, bản sao lưu và lưu trữ trong những thư mục riêng biệt với nhãn được gán gồm tên văn bản và ngày tháng sao lưu.

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.	Có	Có thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ trên ổ cứng di động.