PHỤ LỤC 01

BÁO CÁO KẾT QUẢ TRIỂN KHAI PHƯƠNG ÁN BẢO ĐẢM AN TOÀN THÔNG TIN THEO HỒ SƠ ĐỀ XUẤT CẤP ĐỘ ĐƯỢC PHÊ DUYỆT

I. Thông tin chung

1. Tên cơ quan, đơn vị: UBND xã Hoằng Cát
2. Tên hệ thống thông tin được phê duyệt: Hệ thống thông tin mạng nội bộ tại UBND xã Hoằng Cát
3. Cấp độ hệ thống thông tin được phê duyệt: Cấp độ 1
4. Đầu mối liên hệ:

II. Kết quả triển khai

1. **Đối với các cơ quan đơn vị có Hệ thống thông tin được phê duyệt Hồ sơ đề xuất cấp độ 1**

A. Phương án quản lý

1. Quy định việc xây dựng, cập nhật và sửa đổi Quy chế bảo đảm an toàn thông tin

STT	Nội dung yêu cầu	Tài liệu kiểm chứng
1.1	Ban hành Quyết định phê duyệt Quy chế bảo đảm an toàn thông tin, an ninh mạng trong cơ quan, đơn vị	Quyết định số 126/QĐ-UBND ngày 09 tháng 12 năm 2022 của Ủy ban nhân dân xã Hoằng Cát

2. Quy định về bảo đảm nguồn nhân lực

STT	Nội dung yêu cầu	Tài liệu kiểm chứng
2.1	- Quy định về cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành phù hợp với vị trí tuyển dụng.	Đáp ứng, tham chiếu điều 5 Quy chế bảo đảm an toàn, an ninh mạng: Cán bộ được tuyển dụng, bố trí vào vị trí làm về an toàn thông tin có trình độ, năng lực về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng được lồng ghép trong quy trình tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ.
	- 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;	Đáp ứng, tham chiếu điều 5 Quy chế bảo đảm an toàn, an ninh mạng: Xây dựng kế hoạch và định kỳ hằng năm tổ chức đào tạo hoặc tham gia đào tạo về an toàn thông tin cho 03 nhóm đối tượng bao gồm: cán bộ kỹ thuật, cán bộ quản lý và người sử dụng trong hệ thống.
	- Có hình thức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng;	Đáp ứng, tham chiếu điều 5 Quy chế bảo đảm an toàn, an ninh mạng. - Các bộ phận, cá nhân tham gia sử dụng các dịch vụ của hệ thống phải tuân thủ các quy định về bảo đảm an toàn, an ninh thông tin và chịu trách nhiệm đối với mọi hoạt động trên tài khoản truy cập của mình đã được cấp trên hệ thống. - Phải được thường xuyên tổ chức quán triệt các quy định về ATTT, nhằm nâng cao nhận thức về trách nhiệm đảm bảo ATTT.

	- Cán bộ chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức.	Đáp ứng, tham chiếu điều 5 Quy chế bảo đảm an toàn, an ninh mạng. Quy định đối với cán bộ nghỉ hoặc thay đổi công việc, trong tối đa 05 ngày làm việc: a) Cán bộ nghỉ hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác thuộc sở hữu của tổ chức. b) Cán bộ quản trị phải vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.

3. Quy định về Quản lý thiết kế, xây dựng hệ thống

STT	Nội dung yêu cầu	Tài liệu kiểm chứng
3.1	Thiết kế an toàn hệ thống thông tin: - Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin; - Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.	Đáp ứng, tham chiếu điều 6 chương II Quy chế bảo đảm an toàn, an ninh mạng.
3.2	Thử nghiệm và nghiệm thu hệ thống: - Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng	Đáp ứng, tham chiếu điều 7 chương II Quy chế bảo đảm an toàn, an ninh mạng.

4. Quy định về Quản lý vận hành hệ thống

STT	Nội dung yêu cầu	Tài liệu kiểm chứng
4.1	Quản lý an toàn mạng: - Quản lý vận hành hoạt động bình thường của hệ thống - Cập nhật, sao lưu dự phòng và khôi phục hệ thống sau khi xảy ra sự cố - Truy cập và quản lý cấu hình của hệ thống - Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống trước khi đưa vào vận hành, khai thác	Đáp ứng, tham chiếu điều 8 Chương III Quy chế bảo đảm an toàn, an ninh mạng Quy định về quản lý an toàn mạng: 1. Quản lý, vận hành hoạt động bình thường của hệ thống. a) Thực hiện việc quản lý và kiểm soát mạng nhằm ngăn ngừa các nguy cơ, rủi ro và duy trì an toàn cho các máy tính, ứng dụng sử dụng mạng: - Có sơ đồ logic và vật lý về hệ thống mạng, tổ chức quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý hệ thống chặt chẽ, bảo đảm an toàn và bảo mật. - Sử dụng thiết bị tường lửa, thiết bị phát hiện và kiểm soát truy cập từ bên ngoài mạng và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng; Kiểm soát truy cập từ bên trong mạng; Kết nối về hệ thống giám sát tập trung; Phòng chống xâm nhập giữa các vùng mạng; Phòng chống phần mềm độc hại trên môi trường mạng. b) Thiết lập, cấu hình đầy đủ các tính năng của thiết bị mạng. Thường xuyên, kiểm tra phiên bản hệ điều hành của thiết bị mạng để cập nhật, vá lỗi khi cần thiết. Sử dụng các công cụ để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng bảo mật và các truy cập bất hợp pháp vào hệ thống mạng. Thường xuyên kiểm tra, phát hiện những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào mạng. c) Xác định và ghi rõ các tính năng an toàn, các mức độ bảo mật của dịch vụ và yêu cầu quản lý trong các thỏa thuận về dịch vụ mạng do bên thứ ba cung cấp. d) Mạng không dây (WIFI), thiết lập các thông số an toàn và định kỳ ít nhất 3 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật. Hệ thống mạng không dây phải được bảo vệ bởi mật khẩu

		an toàn. 2. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố - Phải có phương án dự phòng đường truyền mạng, thiết bị mạng để đảm bảo tính sẵn sàng đáp ứng yêu cầu hoạt động của hệ thống mạng. - Triển khai hệ thống/phương tiện lưu trữ độc lập để lưu trữ các thông tin cấu hình thiết bị mạng, kết nối, định danh trong mạng để khôi phục sau khi xảy ra sự cố. 3. Truy cập và quản lý cấu hình hệ thống a) Cán bộ quản lý, nhân viên vận hành truy cập, khai thác thông tin 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. b) Cán bộ quản lý, nhân viên vận hành có trách nhiệm theo dõi và phát hiện các trường hợp truy cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, báo cáo cho cán bộ quản lý để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm. c) Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác. d) 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 (cứng hóa) trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác.
4.2	Quản lý an toàn dữ liệu: - Có phương án sao lưu dự phòng thông tin, dữ liệu, cấu hình hệ thống	Đáp ứng, tham chiếu điều 9 Chương III Quy chế bảo đảm an toàn, an ninh mạng. 5. 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 đơn vị quản lý. 6. Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ. a) 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, dữ liệu, thông tin nghiệp vụ và các thông tin, dữ liệu quan trọng khác trên hệ thống (nếu có). b) Thực hiện sao lưu dữ liệu định kỳ: Cán bộ phụ trách sao lưu thực hiện sao lưu định kỳ theo phương án sao lưu đã được phê duyệt. c) Kiểm tra định kỳ: Dữ liệu sao lưu phải được lưu trữ an toàn và được kiểm tra thường xuyên đảm bảo sẵn sàng cho việc sử dụng khi cần. Kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu.

5. Triển khai Phương án Quản lý rủi ro an toàn thông tin và Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ các thành phần hoặc toàn bộ hệ thống thông tin

STT	Nội dung yêu cầu	Tài liệu kiểm chứng
5.1	Phương án Quản lý rủi ro an toàn thông tin	Đáp ứng, tham chiếu điều 19 Chương IV Quy chế bảo đảm an toàn, an ninh mạng. 1. Xác định mức rủi ro a) Nhận biết tài sản thông qua xác định và thu thập thông tin đầy đủ về tài sản của mình đang quản lý, đặc biệt là các thông tin liên quan đến đặc điểm, nơi lưu trữ, mức độ quan trọng và giá trị, đặc thù của tài sản. Đánh giá các nguy cơ, điểm yếu đối với tài sản đó, từ đó có thể đánh giá xem mỗi tài sản khi gặp rủi ro thì sẽ gây ra hậu quả, mức độ ảnh hưởng thế nào đối với cơ quan, tổ chức b) Phân loại nhóm các điểm yếu: Nhóm các điểm yếu liên quan đến tồn tại lỗ hổng, điểm yếu an toàn thông tin trong hệ thống;

		Nhóm các điểm yếu liên quan đến thiếu hoặc không đáp ứng các biện pháp quản lý: Không có quy định về sử dụng mật khẩu an toàn; không có quy định về lưu trữ có mã hóa, không có quy định về quy trình xử lý sự cố, không có quy định về bảo đảm an toàn thông tin phía người sử dụng.v.v.; Nhóm các điểm yếu liên quan đến thiếu hoặc không đáp ứng các biện pháp kỹ thuật: Không có biện pháp phòng chống xâm nhập, không có biện pháp phòng chống mã độc, không có biện pháp phòng chống tấn công.v.v.; Nhóm các điểm yếu khác liên quan đến các nguy cơ mất an toàn thông tin từ bên thứ ba. c) Phân loại các mối đe dọa: Nhóm các mối đe dọa từ việc tồn tại, điểm yếu, lỗ hổng trong hệ thống; Nhóm các mối đe dọa từ việc thiếu hoặc không đáp ứng các biện pháp quản lý; Nhóm các mối đe dọa từ việc thiếu hoặc không đáp ứng các biện pháp kỹ thuật. d) Đánh giá hậu quả và khả năng xảy ra sự cố, xác định mức rủi ro bao gồm các mức thấp, trung bình, cao, rất cao, cực cao. 2. Quy trình đánh giá và quản lý rủi ro bao gồm 04 bước: (1) Thiết lập bối cảnh; (2) Đánh giá rủi ro; (3) Xử lý rủi ro; (4) Chấp nhận rủi ro và 02 quá trình cần thực hiện song song: Truyền thông và tư vấn rủi ro, Giám sát và soát xét rủi ro. 3. Biện pháp kiểm soát rủi ro được thực hiện theo yêu cầu an toàn cơ bản trong Hồ sơ đề xuất cấp độ của Hệ thống thông tin được cấp có thẩm quyền phê duyệt.
5.2	Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ	Đáp ứng, tham chiếu điều 16 Chương III Quy chế bảo đảm an toàn, an ninh mạng. 1. Khi kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống phải được bộ phận chuyên trách an toàn thông tin thực hiện kiểm tra, đánh giá bảo đảm an toàn thông tin. 2. Quá trình xử lý thông tin trên hệ thống phải được thực hiện khi thay đổi mục đích sử dụng hoặc gỡ bỏ theo phương án kỹ thuật được lãnh đạo UBND xã phê duyệt.

B. Phương án kỹ thuật

1. Yêu cầu về thiết kế hệ thống

STT	Nội dung yêu cầu	Tài liệu kiểm chứng
1.1	Hệ thống mạng phải được thiết kế thành các vùng mạng độc lập theo Hồ sơ cấp độ được phê duyệt, trong đó: - Chỉ sử dụng 01 đường truyền Internet chính với địa chỉ IP tĩnh để cung cấp dịch vụ truy cập Internet cho toàn bộ người dùng trong cơ quan, đơn vị. - Đối với các kết nối mạng có dây từ máy tính người dùng được quy hoạch vào trong phân vùng mạng nội bộ (LAN). - Đối với các kết nối không dây dành cho người sử dụng và khách được quy hoạch vào trong vùng mạng không dây (WIFI). Mạng không dây (WIFI), thiết lập bảo vệ bởi mật khẩu an toàn	- Đã thực hiện phân tách mạng nội bộ (mạng LAN) và mạng không dây (Wifi) tuy nhiên chưa đầy đủ. Dự kiến hoàn thành trong tháng 9/2024
1.2	Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập, sử dụng sản phẩm Tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc phương án tương đương	- Đang thực hiện, tháng 9/2024 hoàn thành.
1.3	Có phương án phòng chống mã độc cho máy trạm sử dụng sản phẩm Phòng chống mã độc hoặc phương án tương đương	- Đang thực hiện, tháng 9/2024 hoàn thành.

2. Yêu cầu về thiết lập, cấu hình hệ thống

STT	Nội dung yêu cầu	Tài liệu kiểm chứng
2.1	Nhật ký hệ thống: Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị mạng chính	- Đang thực hiện, tháng 9/2024 hoàn thành.
2.2	Phòng chống xâm nhập: Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng (Signatures)	- Đang thực hiện, tháng 9/2024 hoàn thành.