

Số: /BC-UBND

Tà Đùng, ngày tháng 6 năm 2026

BÁO CÁO

Rà soát, đánh giá bảo đảm an ninh, an toàn thông tin và việc ứng dụng các phần mềm, ứng dụng công nghệ, chuyển đổi số tại các cơ quan, đơn vị tại xã Tà Đùng

Kính gửi: Công an tỉnh Lâm Đồng (Phòng PA03).

Thực hiện ý kiến chỉ đạo của UBND tỉnh Lâm Đồng về việc rà soát, đánh giá bảo đảm an ninh, an toàn thông tin và việc ứng dụng các phần mềm, ứng dụng công nghệ, chuyển đổi số tại các cơ quan, tổ chức thuộc hệ thống chính trị tại địa phương, UBND xã Tà Đùng báo cáo kết quả rà soát, đánh giá như sau:

I. CĂN CỨ, MỤC ĐÍCH, PHẠM VI RÀ SOÁT

1. Căn cứ thực hiện

- Luật Công nghệ thông tin ngày 29/6/2006; Luật An toàn thông tin mạng ngày 19/11/2015; Luật An ninh mạng ngày 12/6/2018;
- Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;
- Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP;
- Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia;
- Hồ sơ đề xuất cấp độ an toàn hệ thống thông tin đối với Hệ thống mạng nội bộ của UBND xã Tà Đùng; Quy chế bảo đảm an toàn, an ninh mạng Hệ thống cơ sở hạ tầng thông tin mạng nội bộ của UBND xã Tà Đùng ban hành kèm theo Quyết định số 356/QĐ-UBND ngày 07/4/2026.

2. Mục đích

- Đánh giá hiện trạng bảo đảm an ninh, an toàn thông tin đối với hạ tầng mạng, thiết bị công nghệ thông tin, dữ liệu, tài khoản người dùng và quá trình vận hành các hệ thống, phần mềm phục vụ công tác lãnh đạo, chỉ đạo, điều hành tại xã.
- Rà soát mức độ ứng dụng các phần mềm, nền tảng số, ứng dụng công nghệ, chuyển đổi số tại các cơ quan, tổ chức thuộc hệ thống chính trị xã Tà Đùng;

xác định kết quả đạt được, tồn tại, nguyên nhân và nhiệm vụ cần triển khai trong thời gian tới.

- Làm cơ sở đề xuất cấp có thẩm quyền hỗ trợ thẩm định, hướng dẫn kỹ thuật, bố trí nguồn lực để hoàn thiện hồ sơ cấp độ, nâng cao năng lực an toàn thông tin và chuyển đổi số của xã.

3. Phạm vi, đối tượng rà soát

Phạm vi rà soát gồm: hệ thống mạng nội bộ, thiết bị đầu cuối, thiết bị mạng, tài khoản truy cập, dữ liệu, việc sử dụng các phần mềm dùng chung, phần mềm chuyên ngành, nền tảng phục vụ dịch vụ công trực tuyến, điều hành, trao đổi văn bản điện tử của HĐND, UBND, các tổ chức chính trị - xã hội, bộ phận tiếp nhận và trả kết quả, các đơn vị sự nghiệp và các tổ chức, cá nhân có kết nối, sử dụng hệ thống mạng nội bộ của UBND xã Tà Đùng.

II. KẾT QUẢ RÀ SOÁT, ĐÁNH GIÁ

1. Hiện trạng hạ tầng công nghệ thông tin và hệ thống mạng nội bộ

Hệ thống thông tin được rà soát là Hệ thống mạng nội bộ của UBND xã Tà Đùng, do UBND xã Tà Đùng làm chủ quản, đồng thời là đơn vị vận hành; địa chỉ tại Bon Pang So, xã Tà Đùng, tỉnh Lâm Đồng. Hệ thống được thiết lập để kết nối cán bộ, công chức, người lao động và bộ phận tiếp nhận, trả kết quả giải quyết thủ tục hành chính, phục vụ công tác chỉ đạo, điều hành, ứng dụng công nghệ thông tin, khai thác dịch vụ công trực tuyến và phục vụ người dân, doanh nghiệp trên địa bàn xã.

Hạ tầng hiện tại chủ yếu là mạng nội bộ, đường truyền Internet, thiết bị chuyển mạch, thiết bị phát Wi-Fi và máy trạm phục vụ công việc. Hệ thống không triển khai máy chủ riêng, không cung cấp ứng dụng, dịch vụ trực tuyến công khai trên môi trường Internet. Một số ứng dụng, phần mềm phục vụ nghiệp vụ được khai thác theo mô hình dùng chung của tỉnh, của ngành và các hệ thống quốc gia.

Stt	Nội dung rà soát	Hiện trạng/đánh giá
1	Chủ quản, đơn vị vận hành	UBND xã Tà Đùng là chủ quản và đơn vị vận hành hệ thống mạng nội bộ; công chức phụ trách công nghệ thông tin/chuyển đổi số được giao làm đầu mối tham mưu, quản trị, phối hợp bảo đảm an toàn thông tin.
2	Thiết bị mạng đang sử dụng	Có 05 modem/VNPT tại vùng mạng biên, 05 thiết bị chuyển mạch tại vùng mạng nội bộ, 05 thiết bị Wi-Fi phục vụ kết nối không dây. Các thiết bị cần tiếp tục được quản lý cấu hình, thay đổi mật khẩu mặc định, cập nhật bản vá và sao lưu cấu hình định kỳ.
3	Máy chủ, ứng dụng nội bộ	Qua rà soát, hệ thống thông tin của xã không triển khai máy chủ riêng, không cung cấp dịch vụ/ứng

		dụng nội bộ hoặc ứng dụng công khai trên Internet. Đây là yếu tố giúp giảm bề mặt tấn công nhưng vẫn cần quản lý an toàn máy trạm, tài khoản và dữ liệu nghiệp vụ.
4	Quy hoạch kỹ thuật	Hồ sơ đề xuất cấp độ đã xác định định hướng phân tách vùng mạng nội bộ, vùng mạng biên, vùng DMZ, vùng máy chủ nội bộ, vùng mạng không dây và vùng VPN; trang bị/hoàn thiện tường lửa, chuyển mạch lõi, kiểm soát truy cập giữa các vùng mạng.
5	Nhu cầu bổ sung	Cần tiếp tục đầu tư, cấu hình và vận hành thiết bị tường lửa trung tâm, chuyển mạch lõi, cơ chế cân bằng tải/dự phòng đường truyền, phân vùng VLAN, hệ thống ghi nhật ký, phần mềm phòng chống mã độc và phương án sao lưu độc lập.

2. Rà soát, đánh giá bảo đảm an ninh, an toàn thông tin

a) Về hồ sơ cấp độ và quy chế an toàn thông tin

UBND xã Tà Đùng đã lập Hồ sơ đề xuất cấp độ an toàn hệ thống thông tin đối với Hệ thống mạng nội bộ của UBND xã Tà Đùng, đề xuất hệ thống cấp độ 2. Căn cứ đề xuất là hệ thống phục vụ hoạt động nội bộ của cơ quan, có xử lý thông tin riêng, thông tin cá nhân của người sử dụng nhưng không xử lý thông tin bí mật nhà nước theo quy định của pháp luật.

UBND xã đã ban hành Quy chế bảo đảm an toàn, an ninh mạng Hệ thống cơ sở hạ tầng thông tin mạng nội bộ của UBND xã Tà Đùng theo Quyết định số 356/QĐ-UBND ngày 07/4/2026. Quy chế đã quy định phạm vi, đối tượng áp dụng, nguyên tắc bảo đảm an toàn thông tin, các hành vi nghiêm cấm, phối hợp xử lý sự cố, bảo đảm nguồn nhân lực, thiết kế an toàn hệ thống, quản lý an toàn mạng, quản lý dữ liệu, quản lý sự cố và trách nhiệm tổ chức thực hiện.

b) Về tổ chức quản lý, vận hành

- UBND xã đã bố trí công chức phụ trách công nghệ thông tin/an toàn thông tin là đầu mối liên hệ, phối hợp với cơ quan chuyên trách, cơ quan có thẩm quyền trong công tác bảo đảm an toàn thông tin.

- Đã bố trí công chức đầu mối phối hợp xử lý, báo cáo sự cố với Bộ phận thường trực Đội ứng cứu sự cố - Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh Lâm Đồng.

- Định kỳ hằng năm tổ chức hoặc tham gia phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin; tham gia tập huấn, diễn tập an toàn thực chiến do đơn vị có thẩm quyền tổ chức.

- Đã quy định trách nhiệm thu hồi tài sản, vô hiệu hóa quyền truy cập, bàn giao tài sản công nghệ thông tin và cam kết bảo mật khi cán bộ, công chức, viên chức, người lao động chấm dứt hoặc thay đổi công việc.

c) Về biện pháp kỹ thuật

- Định hướng thiết kế an toàn gồm phân vùng mạng, kiểm soát truy cập giữa vùng mạng nội bộ, vùng mạng biên, DMZ, vùng máy chủ nội bộ, vùng mạng không dây, vùng VPN; các kết nối từ bên ngoài vào tài nguyên nội bộ phải thông qua VPN được mã hóa.

- Tường lửa trung tâm được quy hoạch để quản lý truy cập vào/ra, bảo vệ vùng DMZ, vùng máy chủ nội bộ, vùng mạng biên và vùng mạng nội bộ; đồng thời tích hợp hoặc cấu hình chức năng IDS/IPS để phát hiện, ngăn chặn xâm nhập.

- Các thiết bị hệ thống cần bật chức năng ghi nhật ký, đồng bộ thời gian, hạn chế địa chỉ được phép quản trị, sử dụng giao thức quản trị an toàn, không sử dụng giao thức không mã hóa hoặc mã hóa lỗi thời.

- Máy trạm cần được cài đặt phần mềm phòng, chống mã độc, cập nhật bản vá; thiết bị lưu trữ ngoài phải được quét mã độc trước khi đọc hoặc sao chép dữ liệu; mạng Wi-Fi khác phải tách biệt với mạng nội bộ.

- Dữ liệu, cấu hình hệ thống và thông tin nghiệp vụ phải được sao lưu định kỳ hoặc khi có thay đổi; tệp lưu trữ dữ liệu không công khai cần được bảo vệ bằng mật khẩu/mã hóa và kiểm tra tính toàn vẹn.

d) Đánh giá mức độ đáp ứng

Nhóm nội dung	Kết quả đánh giá	Nội dung cần tiếp tục hoàn thiện
Quản lý chính sách, quy chế	Cơ bản đáp ứng: đã ban hành quy chế, xác định trách nhiệm, nguyên tắc, hành vi nghiêm cấm, quản lý người dùng, dữ liệu, sự cố.	Rà soát, cập nhật quy chế định kỳ 03 năm hoặc khi có thay đổi; lưu hồ sơ phản hồi, biên bản triển khai, minh chứng phổ biến đến người dùng.
Tổ chức, nhân lực	Cơ bản đáp ứng: đã phân công đầu mối CNTT/ATTT, đầu mối phối hợp Công an tỉnh, yêu cầu đào tạo nâng cao nhận thức.	Tăng cường đào tạo thực hành, diễn tập xử lý sự cố; xây dựng danh sách tài khoản, tài sản, người quản lý và quy trình bàn giao khi thay đổi nhân sự.
Kỹ thuật mạng	Đã có phương án thiết kế; hiện trạng hạ tầng còn ở mức cơ bản, cần tiếp tục đầu tư theo quy hoạch mới.	Triển khai/hoàn thiện tường lửa, phân vùng VLAN, VPN, ghi nhật ký, cân bằng tải/dự phòng đường truyền, kiểm soát Wi-Fi khách, bảo vệ thiết bị mạng.

Máy chủ, ứng dụng	Không có máy chủ và không cung cấp ứng dụng công khai trên Internet, nguy cơ tấn công trực tiếp vào dịch vụ tự vận hành thấp.	Tiếp tục kiểm soát chặt máy trạm, tài khoản truy cập hệ thống dùng chung, tài khoản quản trị thiết bị mạng; đánh giá cấp độ nếu phát sinh hệ thống/ứng dụng mới.
Dữ liệu, sao lưu	Đã có quy định về sao lưu cấu hình, dữ liệu nghiệp vụ và không xử lý thông tin bí mật nhà nước trên máy tính có Internet.	Lập danh mục dữ liệu, phân loại dữ liệu, lịch sao lưu hàng tháng; kiểm tra khả năng phục hồi, lưu bản sao độc lập và quản lý mật khẩu tệp sao lưu.

3. Rà soát việc ứng dụng phần mềm, ứng dụng công nghệ, chuyển đổi số

Các cơ quan, tổ chức thuộc hệ thống chính trị tại xã đã cơ bản ứng dụng các nền tảng, phần mềm dùng chung và phần mềm chuyên ngành phục vụ công tác lãnh đạo, chỉ đạo, điều hành, giải quyết thủ tục hành chính và trao đổi thông tin. Các hệ thống chủ yếu được vận hành tập trung ở cấp tỉnh, cấp ngành hoặc nền tảng quốc gia; xã sử dụng tài khoản được cấp, máy trạm và đường truyền Internet để truy cập, xử lý công việc.

Stt	Lĩnh vực/phần mềm, nền tảng	Kết quả rà soát, đánh giá
1	Quản lý văn bản, điều hành, thư điện tử công vụ	Cán bộ, công chức sử dụng hệ thống quản lý văn bản và điều hành, thư điện tử công vụ để tiếp nhận, xử lý, phát hành văn bản, trao đổi công việc. Cần tiếp tục nâng cao tỷ lệ xử lý văn bản điện tử, ký số, lập hồ sơ công việc điện tử; hạn chế gửi tài liệu công vụ qua tài khoản cá nhân hoặc nền tảng không được phép.
2	Dịch vụ công trực tuyến, một cửa điện tử	Bộ phận tiếp nhận và trả kết quả sử dụng các hệ thống phục vụ tiếp nhận, luân chuyển, xử lý hồ sơ thủ tục hành chính, hỗ trợ người dân, doanh nghiệp khai thác dịch vụ công trực tuyến. Cần tiếp tục hướng dẫn người dân nộp hồ sơ trực tuyến, thanh toán trực tuyến, theo dõi trạng thái hồ sơ và sử dụng tài khoản định danh điện tử.
3	Cơ sở dữ liệu, phần mềm chuyên ngành	Các bộ phận chuyên môn sử dụng các hệ thống, cơ sở dữ liệu chuyên ngành theo phân quyền của cấp trên trong các lĩnh vực hộ tịch, tài chính, đất đai, văn hóa - xã hội, lao động, thống kê, y tế, giáo dục, an sinh xã hội và lĩnh vực khác. Cần rà soát tài khoản, phân quyền đúng chức năng, cập nhật dữ liệu kịp thời, không chia sẻ tài khoản dùng chung.
4	Chữ ký số, chứng thư số, xác thực điện tử	Việc sử dụng chữ ký số phục vụ phát hành văn bản điện tử và giao dịch điện tử đã được quan tâm triển khai. Cần kiểm tra thời hạn chứng thư số, thiết bị ký

		số, quy trình quản lý khóa bí mật, trách nhiệm của người được cấp và phương án cấp mới, thu hồi khi thay đổi vị trí công tác.
5	Ứng dụng phục vụ truyền thông, tuyên truyền, tương tác với người dân	Các kênh thông tin điện tử, nhóm trao đổi công việc, phương tiện truyền thông số được sử dụng để tuyên truyền chủ trương, chính sách, hướng dẫn dịch vụ công, chuyển đổi số. Cần bảo đảm nội dung đăng tải chính xác, không đưa thông tin bí mật nhà nước, thông tin cá nhân không được phép lên mạng xã hội hoặc nền tảng công khai.
6	An toàn thông tin cho người dùng cuối	Máy tính, thiết bị đầu cuối là điểm truy cập chủ yếu vào các phần mềm, nền tảng số. Cần quản lý danh mục thiết bị, cấu hình bảo mật tối thiểu, cài đặt phần mềm phòng chống mã độc, cập nhật hệ điều hành, trình duyệt, phần mềm văn phòng và thường xuyên nhắc nhở người dùng nhận diện thư giả mạo, liên kết độc hại.
7	Nâng cao kỹ năng số, bình dân học vụ số	Việc hỗ trợ cán bộ, công chức, đoàn thể, tổ công nghệ số cộng đồng và người dân sử dụng dịch vụ số cần được duy trì thường xuyên. Cần lồng ghép nội dung an toàn thông tin, bảo vệ dữ liệu cá nhân, sử dụng tài khoản định danh điện tử, dịch vụ công trực tuyến vào các buổi tập huấn, tuyên truyền.

4. Rà soát theo nhóm cơ quan, tổ chức thuộc hệ thống chính trị tại xã

Nhóm cơ quan, tổ chức	Hiện trạng ứng dụng công nghệ, chuyển đổi số	Yêu cầu bảo đảm an toàn thông tin
UBND xã, các phòng/bộ phận chuyên môn	Ứng dụng phần mềm quản lý văn bản, dịch vụ công, phần mềm chuyên ngành, cơ sở dữ liệu dùng chung, chữ ký số và các nền tảng phục vụ chỉ đạo điều hành.	Kiểm soát tài khoản, phân quyền, ghi nhận bàn giao khi thay đổi nhân sự; bảo vệ máy trạm, dữ liệu nghiệp vụ; chấp hành quy chế an toàn thông tin và quy trình xử lý sự cố.
Trung tâm phục vụ hành chính công/bộ phận tiếp nhận và trả kết quả	Sử dụng các hệ thống một cửa điện tử, dịch vụ công trực tuyến, công cụ hỗ trợ người dân, doanh nghiệp nộp hồ sơ, theo dõi, nhận kết quả.	Bảo vệ dữ liệu cá nhân, hồ sơ thủ tục hành chính; bố trí máy tính công vụ an toàn; không lưu mật khẩu tự động; thường xuyên kiểm tra mã độc trên thiết bị ngoại vi.
Tổ công nghệ số cộng đồng, thôn/bon, lực lượng hỗ trợ chuyển đổi số cơ sở	Tham gia tuyên truyền, hướng dẫn người dân sử dụng dịch vụ công trực tuyến, nền tảng số, tài khoản định danh điện tử,	Tuyên truyền an toàn thông tin, bảo vệ dữ liệu cá nhân; hướng dẫn người dân không cung cấp mã OTP, mật khẩu, thông tin cá nhân cho

	thanh toán số và kỹ năng số cơ bản.	đối tượng lạ; phát hiện, báo cáo kịp thời tin giả, lừa đảo trực tuyến.
--	-------------------------------------	--

III. NHẬN XÉT, ĐÁNH GIÁ CHUNG

1. Kết quả đạt được

- Công tác bảo đảm an toàn thông tin, an ninh mạng đã được quan tâm chỉ đạo; xã đã có hồ sơ đề xuất cấp độ, quy chế bảo đảm an toàn, an ninh mạng và phân công đầu mối phụ trách công nghệ thông tin/chuyển đổi số.

- Các phần mềm dùng chung, hệ thống chuyên ngành, dịch vụ công trực tuyến được khai thác để phục vụ chỉ đạo điều hành, giải quyết thủ tục hành chính, trao đổi văn bản điện tử, từng bước giảm giấy tờ và nâng cao hiệu quả phục vụ người dân, doanh nghiệp.

- Nhận thức của cán bộ, công chức về chuyển đổi số và an toàn thông tin từng bước được nâng lên; việc sử dụng chữ ký số, thư điện tử công vụ, văn bản điện tử, hồ sơ trực tuyến được duy trì và mở rộng.

- Hệ thống hiện không cung cấp dịch vụ công khai trên Internet và không vận hành máy chủ riêng, do đó giảm được nguy cơ tấn công trực tiếp vào các máy chủ/ứng dụng do xã tự quản; trọng tâm bảo vệ chuyển sang máy trạm, tài khoản, dữ liệu và thiết bị mạng.

2. Tồn tại, hạn chế

- Hạ tầng mạng hiện tại còn phân tán, thiết bị bảo mật chuyên dụng, chuyển mạch lõi, phân vùng mạng, giám sát nhật ký, cân bằng tải và dự phòng đường truyền cần tiếp tục được đầu tư, cấu hình đồng bộ theo hồ sơ đề xuất cấp độ.

- Chưa có cán bộ chuyên trách an toàn thông tin làm việc toàn thời gian; năng lực xử lý sự cố, đánh giá rủi ro, quản trị cấu hình nâng cao còn phụ thuộc nhiều vào sự hỗ trợ của cơ quan chuyên môn cấp trên và nhà cung cấp dịch vụ.

- Danh mục tài sản thông tin, dữ liệu, tài khoản, thiết bị đầu cuối, thiết bị mạng và minh chứng sao lưu, kiểm tra phục hồi cần được cập nhật thường xuyên hơn để đáp ứng yêu cầu quản lý rủi ro và kiểm tra, đánh giá định kỳ.

- Nguy cơ mất an toàn thông tin từ người dùng cuối vẫn còn: sử dụng thiết bị cá nhân, USB, mật khẩu yếu, lưu mật khẩu tự động, truy cập liên kết lạ, dùng nhóm mạng xã hội để trao đổi tài liệu công vụ hoặc chia sẻ thông tin cá nhân không đúng quy định.

- Việc ứng dụng phần mềm, nền tảng số phụ thuộc vào hạ tầng đường truyền, tài khoản phân quyền và hệ thống dùng chung của cấp trên; khi hệ thống

tập trung bị lỗi hoặc đường truyền không ổn định sẽ ảnh hưởng đến hoạt động của xã.

3. Nguyên nhân

- Nguồn lực đầu tư cho hạ tầng công nghệ thông tin, an toàn thông tin ở cấp xã còn hạn chế; trang thiết bị từng giai đoạn chưa đồng bộ, chưa đáp ứng đầy đủ yêu cầu phân vùng, giám sát và dự phòng theo tiêu chuẩn kỹ thuật.

- Cán bộ phụ trách công nghệ thông tin phải kiêm nhiệm nhiều nhiệm vụ; công nghệ, quy định và phương thức tấn công mạng thay đổi nhanh, đòi hỏi phải thường xuyên được đào tạo, cập nhật.

- Một bộ phận người dùng còn thói quen xử lý hồ sơ, trao đổi tài liệu theo phương thức truyền thống hoặc sử dụng công cụ tiện lợi nhưng chưa bảo đảm yêu cầu bảo mật.

- Công tác lập hồ sơ minh chứng, kiểm tra định kỳ, đánh giá rủi ro, diễn tập khôi phục sau sự cố chưa được duy trì thường xuyên theo chu kỳ.

IV. NHIỆM VỤ, GIẢI PHÁP TRONG THỜI GIAN TỚI

1. Hoàn thiện hồ sơ, quy chế, quy trình quản lý

- Theo dõi kết quả thẩm định, phê duyệt hồ sơ đề xuất cấp độ an toàn hệ thống thông tin đối với Hệ thống mạng nội bộ của UBND xã Tà Đùng; tổ chức triển khai đầy đủ các yêu cầu quản lý, kỹ thuật tương ứng cấp độ 2 sau khi được phê duyệt.

- Rà soát, cập nhật quy chế, quy trình vận hành, quy trình sao lưu, quy trình xử lý sự cố, quy trình quản lý tài khoản, thiết bị và tài sản thông tin; lập sổ theo dõi minh chứng thực hiện.

- Xây dựng danh mục tài sản thông tin, danh mục dữ liệu, danh mục thiết bị, danh mục tài khoản sử dụng các phần mềm, nền tảng số; phân loại mức độ quan trọng và trách nhiệm quản lý đối với từng nhóm tài sản.

2. Hoàn thiện hạ tầng kỹ thuật và biện pháp bảo vệ

- Ưu tiên trang bị, cấu hình tường lửa trung tâm, chuyển mạch lõi, phân vùng VLAN theo phòng, bộ phận, vùng Wi-Fi khách, vùng VPN; thiết lập nguyên tắc mặc định từ chối các luồng truy cập không được định nghĩa.

- Thiết lập cơ chế cân bằng tải hoặc dự phòng đường truyền Internet; sao lưu cấu hình thiết bị mạng, lưu trữ bản sao độc lập, kiểm tra khả năng phục hồi cấu hình sau sự cố.

- Bật ghi nhật ký trên thiết bị mạng, tường lửa, máy trạm; đồng bộ thời gian; lưu nhật ký tối thiểu theo yêu cầu; định kỳ kiểm tra dấu hiệu bất thường, kết nối lạ, truy cập trái phép hoặc mã độc.

- Cài đặt, cập nhật phần mềm phòng, chống mã độc trên toàn bộ máy trạm; cập nhật hệ điều hành, trình duyệt, phần mềm văn phòng; tắt dịch vụ không cần thiết, hạn chế quyền quản trị cục bộ.

- Thiết lập quy trình kiểm tra USB, ổ cứng di động, thiết bị cá nhân trước khi kết nối vào máy tính công vụ; không sử dụng thiết bị cá nhân để lưu, sao chép tài liệu công vụ khi chưa được phép.

3. Nâng cao hiệu quả ứng dụng phần mềm, nền tảng số

- Tăng cường sử dụng hệ thống quản lý văn bản, điều hành, ký số, thư điện tử công vụ; xử lý văn bản, hồ sơ công việc trên môi trường điện tử theo quy định.

- Đẩy mạnh hướng dẫn người dân sử dụng dịch vụ công trực tuyến, tài khoản định danh điện tử, thanh toán trực tuyến, tra cứu hồ sơ; phát huy vai trò tổ công nghệ số cộng đồng trong hỗ trợ người dân tại thôn/bon.

- Thường xuyên rà soát tài khoản phần mềm chuyên ngành, kịp thời đề nghị cấp mới, điều chỉnh, khóa tài khoản khi có thay đổi nhân sự; không sử dụng tài khoản chung hoặc chia sẻ mật khẩu.

- Thực hiện chuẩn hóa, cập nhật dữ liệu trên các cơ sở dữ liệu chuyên ngành; khai thác dữ liệu đúng mục đích, đúng thẩm quyền; bảo vệ dữ liệu cá nhân, dữ liệu nghiệp vụ theo quy định.

4. Tuyên truyền, đào tạo, kiểm tra và xử lý sự cố

- Hằng năm tổ chức hoặc tham gia các lớp tập huấn về kỹ năng số, an toàn thông tin, an ninh mạng, nhận diện lừa đảo trực tuyến, bảo vệ dữ liệu cá nhân, sử dụng mật khẩu mạnh và xác thực an toàn.

- Tổ chức kiểm tra định kỳ việc chấp hành quy chế an toàn thông tin tại các bộ phận; nhắc nhở, chấn chỉnh kịp thời việc sử dụng thiết bị, tài khoản, phần mềm, dữ liệu và nền tảng mạng xã hội trong xử lý công vụ.

- Thiết lập đầu mối tiếp nhận cảnh báo, sự cố; khi phát hiện dấu hiệu mất an toàn thông tin phải cô lập, ghi nhận hiện trạng, sao lưu thông tin cần thiết và liên hệ ngay cơ quan chuyên trách để phối hợp xử lý.

- Lồng ghép tuyên truyền an toàn thông tin trong hoạt động chuyển đổi số, bình dân học vụ số, sinh hoạt thôn/bon; hướng dẫn người dân không cung cấp OTP, mật khẩu, mã định danh, thông tin tài khoản ngân hàng cho đối tượng lạ.

V. KIẾN NGHỊ, ĐỀ XUẤT

- Đề nghị Sở Khoa học và Công nghệ tỉnh Lâm Đồng hướng dẫn chuyên môn, hỗ trợ đánh giá, kiểm tra, hoàn thiện hồ sơ cấp độ; hỗ trợ tập huấn, chuyển giao tài liệu mẫu về quản lý rủi ro, quản lý tài sản thông tin, quản trị tài khoản, sao lưu và khôi phục dữ liệu.

- Đề nghị Công an tỉnh Lâm Đồng quan tâm thẩm định, phê duyệt hồ sơ đề xuất cấp độ hệ thống thông tin; thường xuyên cung cấp cảnh báo sớm về điểm yếu, lỗ hổng, chiến dịch tấn công mạng, lừa đảo trực tuyến; hỗ trợ xã khi xảy ra sự cố an toàn thông tin.

- Đề nghị các sở, ngành cấp tỉnh tiếp tục hoàn thiện, nâng cấp các phần mềm dùng chung, phần mềm chuyên ngành; bảo đảm tính ổn định, liên thông, phân quyền rõ ràng; có hướng dẫn thống nhất về quản lý tài khoản, khai thác dữ liệu và bảo vệ thông tin cá nhân.

- Đề nghị cấp có thẩm quyền xem xét bố trí kinh phí để UBND xã Tà Đùng đầu tư tường lửa, chuyển mạch lõi, phần mềm phòng chống mã độc, thiết bị lưu trữ sao lưu, nâng cấp đường truyền, bảo trì thiết bị và tổ chức tập huấn an toàn thông tin, chuyển đổi số cho cán bộ, công chức, lực lượng hỗ trợ chuyển đổi số cơ sở.

Trên đây là Báo cáo rà soát, đánh giá bảo đảm an ninh, an toàn thông tin và việc ứng dụng các phần mềm, ứng dụng công nghệ, chuyển đổi số tại các cơ quan, tổ chức thuộc hệ thống chính trị tại xã Tà Đùng. UBND xã Tà Đùng kính báo cáo các cơ quan xem xét, hướng dẫn, phối hợp thực hiện./.

Nơi nhận:

- Như trên;
- Thường trực Đảng ủy xã;
- Thường trực HĐND xã;
- Chủ tịch, các PCT UBND xã;
- Các cơ quan, đơn vị liên quan;
- Lưu: VT, VHXH.

**KT. CHỦ TỊCH
PHÓ CHỦ TỊCH**

Lê Văn Đại