

KẾ HOẠCH

Ứng cứu sự cố an toàn thông tin, an ninh mạng trên địa bàn xã Sơn Tây Thượng

Thực hiện Quyết định số 1744/QĐ-UBND ngày 03/12/2025 của Chủ tịch UBND tỉnh Quảng Ngãi về việc ban hành Phương án ứng cứu sự cố an toàn thông tin, an ninh mạng tỉnh Quảng Ngãi; Quyết định số 860/QĐ-UBND ngày 14/11/2025 của UBND xã Sơn Tây Thượng về việc ban hành Quy chế bảo đảm an toàn thông tin và bảo mật dữ liệu của UBND xã Sơn Tây Thượng. UBND xã Sơn Tây Thượng ban hành Kế hoạch ứng cứu sự cố an toàn thông tin, an ninh mạng trên địa bàn xã Sơn Tây Thượng để cơ quan, đơn vị, cá nhân có liên quan thực hiện như sau:

I. MỤC ĐÍCH, YÊU CẦU VÀ NGUYÊN TẮC CHUNG

1. Mục đích

- Chủ động phát hiện sớm, khoanh vùng, ngăn chặn kịp thời và xử lý hiệu quả các sự cố gây mất an toàn thông tin (ATTT), an ninh mạng (ANM) đối với hệ thống thông tin của UBND xã Sơn Tây Thượng.

- Hạn chế tối đa thiệt hại về dữ liệu chuyên môn, dữ liệu cá nhân của cán bộ và công dân; bảo đảm tính liên tục trong công tác chỉ đạo, điều hành của Lãnh đạo xã và tiếp nhận, giải quyết thủ tục hành chính tại Trung tâm Phục vụ Hành chính công xã.

2. Yêu cầu

- Bám sát Phương án ứng cứu sự cố ATTT, ANM của UBND tỉnh Quảng Ngãi (Quyết định số 1744/QĐ-UBND ngày 03/12/2025) và Quy chế bảo đảm an toàn thông tin của UBND xã (Quyết định số 860/QĐ-UBND ngày 14/11/2025).

- Nội dung phương án ngắn gọn, rõ người, rõ việc, dễ triển khai vận hành; phù hợp với điều kiện cơ sở hạ tầng mạng và nguồn lực thực tế tại xã miền núi Sơn Tây Thượng.

3. Nguyên tắc ứng cứu

- **Nguyên tắc ưu tiên xử lý:** Thực hiện phương châm "4 tại chỗ" (Chỉ đạo tại chỗ, lực lượng tại chỗ, phương tiện tại chỗ, hậu cần tại chỗ). Ưu tiên xử lý nhanh chóng bằng lực lượng tại chỗ, đồng thời kịp thời liên hệ, phối hợp với lực lượng chuyên trách cấp trên khi vượt quá khả năng xử lý.

- **Nguyên tắc an toàn:** Khoanh vùng, cách ly nguồn lây nhiễm trước; bảo vệ an toàn các hệ thống, máy trạm chưa bị ảnh hưởng; ưu tiên phục hồi các dịch vụ hành chính phục vụ người dân và chỉ đạo điều hành khẩn cấp.

- **Nguyên tắc bảo toàn hiện trường:** Trong quá trình xử lý sự cố, cán bộ kỹ thuật phải giữ nguyên hiện trạng kỹ thuật, không tự ý tắt máy đột ngột làm

mất bộ nhớ tạm (RAM) phục vụ công tác giám định, trích xuất log dấu vết tấn công.

II. ĐẶC ĐIỂM HỆ THỐNG VÀ NGUY CƠ ĐẶC THÙ TẠI ĐỊA BÀN

1. Đặc điểm hệ thống thông tin xã Sơn Tây Thượng (Cấp độ 2)

Hệ thống thông tin UBND xã Sơn Tây Thượng vận hành tại Trụ sở cơ quan (tòa nhà 03 tầng) với quy mô gồm 41 máy trạm, 06 bộ phát Wifi, 09 camera an ninh, 01 Router cân bằng tải Ruijie, 01 Tường lửa phần cứng Sophos XGS và các bộ chuyển mạch Switch tầng.

Đặc thù kỹ thuật: UBND xã không triển khai máy chủ dữ liệu (Server) dùng riêng tại trụ sở. Toàn bộ các ứng dụng nghiệp vụ như: Quản lý văn bản và điều hành (iOffice), Cổng Dịch vụ công trực tuyến, CSDL Quốc gia về dân cư (Đề án 06), Quản lý CBCC, Thư điện tử công vụ đều vận hành tập trung trên nền tảng điện toán đám mây dùng chung của tỉnh và của Bộ, ngành.

2. Các nguy cơ sự cố chủ yếu tại địa bàn

- **Nguy cơ hạ tầng, thiên tai:** Do đặc thù xã miền núi vùng cao, thời tiết giông lốc, mưa bão thường gây sự cố chập sét, sụt áp làm hư hỏng thiết bị mạng hoặc gây sạt lở đứt cáp quang viễn thông, làm tê liệt đường truyền liên lạc diện rộng.

- **Nguy cơ mã độc xâm nhập qua thiết bị đầu cuối:** Lây nhiễm mã độc tống tiền (Ransomware), virus qua việc cắm thiết bị lưu trữ di động (USB), mở tệp đính kèm thư rác giả mạo hoặc truy cập các liên kết độc hại do thói quen của một bộ phận người sử dụng.

- **Nguy cơ chiếm đoạt tài khoản tác nghiệp:** Lộ lọt thông tin đăng nhập tài khoản iOffice, tài khoản Dịch vụ công, chữ ký số chuyên dùng công vụ dẫn đến nguy cơ bị can thiệp trái phép, phát tán văn bản sai lệch.

- **Nguy cơ từ thiết bị IoT và mạng không dây:** Tấn công rà quét điểm yếu cổng mạng từ mạng Wifi khách (vùng tiếp dân) hoặc thiết bị camera an ninh lây lan vào vùng mạng nội bộ do chưa quản lý chặt chính sách VLAN.

III. PHÂN LOẠI MỨC ĐỘ SỰ CỐ VÀ CHỈ TIÊU THỜI GIAN XỬ LÝ

Bám sát Quy chuẩn kỹ thuật và Phương án của tỉnh, các sự cố an toàn thông tin tại xã Sơn Tây Thượng được phân làm 03 mức độ ([*theo phụ lục đính kèm*](#)).

IV. QUY TRÌNH ỨNG CỨU SỰ CỐ (05 BƯỚC THỰC HIỆN)

Bước 1: Tiếp nhận thông tin và phát hiện sự cố

- Người sử dụng (cán bộ, công chức, viên chức) khi phát hiện dấu hiệu bất thường trên máy tính cá nhân (màn hình khóa, tệp tin bị đổi đuôi lạ, máy chạy chậm đột biến, tài khoản tự động gửi email, không truy cập được mạng nội bộ...) phải dừng ngay mọi thao tác.

- Thông báo ngay bằng điện thoại hoặc trực tiếp cho Chuyên viên phụ trách CNTT & CDS hoặc Lãnh đạo Phòng Văn hóa - Xã hội; đồng thời báo cáo Lãnh đạo phòng/ban quản lý trực tiếp.

Bước 2: Phân loại sự cố và thực hiện biện pháp phản ứng khẩn cấp tại chỗ

- Cô lập thiết bị ngay lập tức: Rút dây mạng LAN hoặc ngắt hoàn toàn kết nối Wifi đối với máy tính nghi ngờ bị nhiễm mã độc. Tuyệt đối không cắm lại kết nối khi chưa được kiểm tra.

- Không tắt nguồn đột ngột (Hard Shutdown): Không rút dây nguồn máy tính để bảo toàn dữ liệu trên bộ nhớ RAM, phục vụ việc truy xuất dấu vết mã độc.

- Khoanh vùng mạng: Trong trường hợp mã độc lây lan nhanh hoặc nghi ngờ xâm nhập diện rộng, Chuyên viên CNTT chủ động khóa các cổng VLAN tương ứng trên Tường lửa/Switch hoặc ngắt mạng toàn bộ khu vực bị ảnh hưởng.

- Chuyển đổi phương thức làm việc: Trung tâm Phục vụ Hành chính công và Văn thư chuyển sang tiếp nhận hồ sơ giấy hoặc sử dụng thiết bị kết nối 4G/5G độc lập để xử lý các công việc cấp bách, không làm gián đoạn phục vụ nhân dân.

Bước 3: Báo cáo chỉ đạo và đề xuất lực lượng hỗ trợ kỹ thuật

- Đối với sự cố Mức 1: Chuyên viên CNTT lập nhật ký ghi nhận, tiến hành quét diệt mã độc, xử lý tại chỗ và báo cáo kết quả cho Trưởng phòng VH-XH.

- Đối với sự cố Mức 2 và Mức 3: Chuyên viên CNTT báo cáo ngay cho phòng VH-XH, Công an xã để báo cáo Chủ tịch UBND xã; đồng thời kích hoạt kênh thông tin khẩn cấp liên hệ với Phòng An ninh mạng và PCTP sử dụng công nghệ cao (PA05) - Công an tỉnh Quảng Ngãi và Đội Ứng cứu sự cố tỉnh đề nghị cử chuyên gia hỗ trợ.

- Thu thập và bảo quản các tệp tin nhật ký (log) của Tường lửa Sophos XGS, Router Ruijie và bản chụp màn hình để bàn giao cho cơ quan chuyên trách

Bước 4: Xử lý, bóc gỡ mã độc và khôi phục hoạt động hệ thống

- Phối hợp với lực lượng kỹ thuật chuyên trách tỉnh thực hiện bóc gỡ mã độc, vá các lỗ hổng phần mềm trên máy tính bị nhiễm.

- Tiến hành đổi toàn bộ mật khẩu quản trị mạng, mật khẩu tài khoản điều hành iOffice, hòm thư công vụ và tài khoản Cổng Dịch vụ công của các cá nhân liên quan.

- Khôi phục dữ liệu chuyên môn từ các bản sao lưu độc lập (đã lưu trữ định kỳ hàng tuần ra ổ cứng ngoài theo Quy chế 860/QĐ-UBND).

- Kiểm tra quét sạch mã độc toàn diện trước khi cấp quyền đấu nối trở lại vào mạng LAN cơ quan.

Bước 5: Đánh giá, lập biên bản kết thúc và rút kinh nghiệm

- Phòng Văn hóa - Xã hội, Công an xã lập Biên bản sự cố và Báo cáo kết quả khắc phục gửi UBND tỉnh, Sở KH&CN và Công an tỉnh (PA05) theo đúng quy định.

- Rà soát, cập nhật các lỗ hổng an ninh mạng, bổ sung chính sách ngăn chặn trên Tường lửa Sophos XGS và phổ biến bài học kinh nghiệm đến toàn thể cán bộ cơ quan.

V. PHÂN CÔNG TRÁCH NHIỆM

1. Chủ tịch UBND xã: Chỉ đạo toàn diện công tác ứng cứu sự cố ATTT, ANM; quyết định huy động các nguồn lực tại chỗ hoặc đề nghị cơ quan cấp trên tăng cường hỗ trợ kỹ thuật khi xảy ra tình huống nghiêm trọng.

2. Phòng Văn hóa - Xã hội: Là cơ quan chuyên trách tham mưu thường trực; Trưởng phòng trực tiếp điều hành công tác ứng phó sự cố; chỉ đạo Chuyên viên CNTT & CDS triển khai các biện pháp kỹ thuật; tổng hợp báo cáo Lãnh đạo xã và cơ quan cấp trên.

3. Văn phòng HĐND & UBND xã: Phối hợp thông báo nhanh cho các bộ phận; bảo đảm nguồn lực tài chính, hậu cần và cơ sở vật chất phục vụ khắc phục sự cố.

4. Công an xã Sơn Tây Thượng: Phối hợp với Phòng VH-XH và PA05 Công an tỉnh trong việc bảo vệ hiện trường thiết bị, xác minh các dấu hiệu tội phạm mạng và bảo đảm an ninh trật tự công sở.

5. Cán bộ, công chức, người lao động: Nghiêm túc chấp hành các quy định về ATTT; không tự ý đấu nối thiết bị lạ vào mạng nội bộ; chủ động đổi mật khẩu định kỳ và phối hợp chặt chẽ khi có sự cố xảy ra.

Trong quá trình thực hiện, nếu có khó khăn, vướng mắc phát sinh, các đơn vị, cá nhân kịp thời phản ánh về Phòng Văn hóa - Xã hội, Công an xã để tổng hợp, báo cáo Chủ tịch UBND xã xem xét sửa đổi, bổ sung cho phù hợp./.

Nơi nhận:

- TT Đảng ủy;
- Công an xã;
- Phòng VH-XH;
- Cơ quan, đơn vị thuộc xã;
- CT, PCT UBND xã;
- Trưởng thôn;
- Lưu VT.

CHỦ TỊCH



Phạm Hồng Khuyến

