ỦY BAN NHÂN DÂN PHƯỜNG HOÀI NHƠN NAM	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 68 /KH-UBND	*Hoài Nhơn Nam, ngày 30 tháng 3 năm 2026*

KẾ HOẠCH
Ứng phó sự cố, bảo đảm an toàn thông tin mạng UBND phường Hoài Nhơn Nam năm 2026

Căn cứ Luật Tổ chức Chính quyền địa phương ngày 16/6/2025;

Căn cứ Luật Công nghệ thông tin ngày 29/6/2006;

Căn cứ Luật An toàn thông tin mạng ngày 19/11/2015;

Căn cứ Luật An ninh mạng ngày 12/6/2018;

Căn cứ 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;

Căn cứ Nghị định số 13/2018/NĐ-CP ngày 23/01/2018 của Chính phủ quy định chi tiết và biện pháp thi hành Luật Tiếp cận thông tin;

Căn cứ Nghị định số 42/2022/NĐ-CP ngày 24/6/2022 của Chính phủ quy định về cung cấp thông tin và dịch vụ công trực tuyến của cơ quan nhà nước trên môi trường mạng;

Căn cứ Nghị định 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về Bảo vệ dữ liệu cá nhân;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông quy định điều phối, ứng cứu sự cố an toàn thông tin mạng;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông về Quy định chi tiết và hướng dẫn một số điều của 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;

Căn cứ Quyết định số 02/2026/QĐ-UBND ngày 08/01/2026 của UBND tỉnh Gia Lai Ban hành Quy chế bảo đảm an toàn thông tin, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Gia Lai;

Căn cứ Quyết định số 766/QĐ-UBND ngày 22/8/2025 của UBND phường Hoài Nhơn Nam Ban hành Quy chế bảo đảm an toàn, an ninh mạng Hệ thống thông tin nội bộ UBND phường Hoài Nhơn Nam.

UBND phường Hoài Nhơn Nam ban hành Kế hoạch ứng phó sự cố, bảo đảm an toàn thông tin mạng UBND phường Hoài Nhơn Nam năm 2026, cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích:

- Bảo đảm ATTT cho các hệ thống thông tin (HTTT) của phường, đặc biệt là Trang thông tin điện tử (TTĐT), hệ thống Quản lý văn bản và Điều hành, hệ thống Một cửa điện tử, nhằm duy trì tính liên tục của hoạt động chỉ đạo, điều hành và giải quyết thủ tục hành chính (TTHC) cho người dân, doanh nghiệp.

- Bảo đảm an toàn thông tin cho các hệ thống thông tin quan trọng trên địa bàn; bảo đảm khả năng thích ứng chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa mất an toàn thông tin trên mạng, kịp thời khắc phục các tồn tại, lỗ hổng, điểm yếu nhằm phòng ngừa các sự cố tấn công mạng; đề ra các giải pháp ứng phó khi gặp sự cố mất an toàn thông tin mạng.

- Chuẩn bị các nguồn lực và điều kiện cần thiết để sẵn sàng, chủ động ứng phó kịp thời và hiệu quả khi xảy ra sự cố ATTT mạng, giảm thiểu tối đa thiệt hại.

- Xây dựng, phát triển Đội ứng cứu sự cố an toàn thông tin mạng có đầy đủ kiến thức, kỹ năng xử lý sự cố an toàn thông tin mạng bảo đảm linh hoạt, hiệu quả, phù hợp với yêu cầu thực tế.

- Nâng cao nhận thức và kỹ năng thực tế cho cán bộ, công chức (CBCC) của phường, đặc biệt là các lực lượng nòng cốt, về quy trình xử lý và phối hợp khi có sự cố.

- Bảo đảm các nguồn lực và các điều kiện cần thiết để sẵn sàng triển khai kịp thời, hiệu quả các phương án ứng cứu khẩn cấp sự cố an toàn thông tin mạng

- Thiết lập cơ chế phối hợp rõ ràng, mạch lạc giữa các lực lượng tại chỗ của phường và với Đội ứng cứu sự cố ATTT mạng tỉnh Gia Lai.

2. Yêu cầu:

- Quán triệt phương châm "4 tại chỗ": Chỉ huy tại chỗ, lực lượng tại chỗ, phương tiện tại chỗ và hậu cần tại chỗ. Lực lượng tại chỗ phải là nòng cốt trong việc phát hiện, xử lý ban đầu.

- Các hệ thống thông tin của các phòng ban, ngành của phường phải được đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin (ATTT) mạng, dự báo các nguy cơ, sự cố, tấn công mạng có thể xảy ra để đưa ra phương án ứng phó, ứng cứu sự cố kịp thời, phù hợp.

- Chuyển từ bị động ứng phó sang chủ động phòng ngừa, bao gồm việc chủ động rà quét, săn lùng mối nguy và khắc phục sớm các lỗ hổng, điểm yếu.

- Phân định rõ ràng chức năng, nhiệm vụ, trách nhiệm và quyền hạn (rõ người, rõ việc) cho từng cá nhân, bộ phận tham gia vào quy trình ứng cứu.

- Mọi hoạt động ứng cứu phải tuân thủ quy trình kỹ thuật, đảm bảo nguyên tắc bảo mật thông tin, bảo vệ hiện trường (log, chứng cứ số) để phục vụ điều tra khi cần thiết.

- Thường xuyên trao đổi thông tin, chia sẻ kinh nghiệm trong công tác bảo đảm ATTT giữa các cơ quan nhà nước trên địa bàn phường; tận dụng sự phối hợp, hỗ trợ của cơ quan điều phối quốc gia về ứng cứu sự cố (Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT).

II. PHẠM VI, NGUYÊN TẮC VÀ PHÂN LOẠI SỰ CỐ

1. Phạm vi áp dụng:

Kế hoạch này để ứng phó sự cố, bảo đảm an toàn thông tin mạng đối với các hệ thống thông tin của phường, áp dụng cho các phòng, ban, ngành, doanh nghiệp nhà nước; các cơ quan, đơn vị, doanh nghiệp có liên quan (gọi tắt là cơ quan, đơn vị) đến hoạt động ứng cứu sự cố an toàn thông tin mạng trên địa bàn phường.

2. Nguyên tắc ứng phó:

- Tuân thủ các quy định pháp luật về điều phối, ứng cứu sự cố ATTT mạng.

- Chủ động, kịp thời, nhanh chóng, chính xác; phối hợp chặt chẽ, đồng bộ và hiệu quả giữa các cơ quan, đơn vị.

- Ứng cứu sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản hệ thống thông tin.

- Thông tin trao đổi trong mạng lưới ứng phó sự cố ATTT mạng phải được kiểm tra, xác thực đối tượng trước khi thực hiện các bước tác nghiệp tiếp theo.

- Bảo đảm bí mật thông tin khi tham gia, thực hiện các hoạt động ứng cứu sự cố theo yêu cầu của cơ quan điều phối quốc gia hoặc cơ quan, tổ chức, cá nhân gặp sự cố.

3. Các lực lượng tham gia ứng phó sự cố

- Các phòng, ban, doanh nghiệp có liên quan.

- Tổ Ứng cứu Công nghệ và Nghiệp vụ hỗ trợ giải quyết TTHC phường (lực lượng chính ứng phó sự cố).

- Chủ quản hệ thống thông tin; đơn vị quản lý, vận hành hệ thống thông tin.

- Tổ Công nghệ số cộng đồng phường.

- Doanh nghiệp cung cấp dịch vụ viễn thông internet (VNPT, Viettel, FPT, Mobifone,...).

- Doanh nghiệp cung cấp dịch vụ ATTT mạng (trường hợp thuê dịch vụ).

- Trong trường hợp cần thiết, mời các cơ quan chức năng về ứng cứu sự cố cùng tham gia (Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Gia Lai).

4. Chức năng, nhiệm vụ, trách nhiệm và cơ chế, quy trình phối hợp giữa các cơ quan, đơn vị.

- Tổ Ứng cứu Công nghệ và Nghiệp vụ hỗ trợ giải quyết TTHC: Đơn vị chuyên trách về ATTT tại phường, lực lượng chính tham gia các hoạt động ứng cứu sự cố ATTT mạng; thực hiện nhiệm vụ theo Quy chế hoạt động của Tổ; tham gia hoạt động ứng cứu khẩn cấp bảo đảm ATTT mạng quốc gia.

- Tổ công tác về phát triển khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số và Cải cách hành chính: Phối hợp xây dựng, thực thi các quy định về an toàn bảo mật thông tin mạng, quản lý, khai thác và vận hành Cổng thông tin điện tử phường; xử lý, ứng cứu các sự cố về an toàn thông tin, an ninh mạng xảy ra trên địa bàn phường khi có yêu cầu của đơn vị điều phối.

- Công an phường: Phối hợp tổ chức triển khai hoạt động ứng phó sự cố ATTT mạng và các nhiệm vụ khác khi xảy ra sự cố.

- Các cơ quan, đơn vị: Triển khai các nhiệm vụ theo chức năng, nhiệm vụ của đơn vị quản lý, vận hành hệ thống thông tin; Phối hợp với đơn vị chuyên trách ứng cứu sự cố ATTT mạng của phường trong công tác ứng phó, xử lý các sự cố.

- Doanh nghiệp cung cấp, xây dựng các hệ thống thông tin: Phối hợp với đơn vị chuyên trách, Công an phường, chủ quản hệ thống thông tin, đơn vị quản lý, vận hành hệ thống thông tin trong công tác ứng phó, xử lý các sự cố ATTT liên quan hệ thống thông tin do mình xây dựng hoặc cung cấp.

- Doanh nghiệp cung cấp dịch vụ viễn thông internet: Phối hợp với đơn vị chuyên trách, Công an phường, chủ quản hệ thống thông tin, đơn vị quản lý, vận hành hệ thống thông tin trong công tác ứng phó, xử lý các sự cố ATTT liên quan đến hạ tầng viễn thông, dịch vụ Internet do mình cung cấp hoặc quản lý.

3. Phân loại sự cố: Tổ Ứng cứu Công nghệ và Nghiệp vụ hỗ trợ giải quyết TTHC phường chịu trách nhiệm phân loại ban đầu để quyết định mức độ phản ứng:

- Mức 1 (Thấp): Sự cố ảnh hưởng đến 01 máy, không lây lan, không ảnh hưởng trực tiếp đến dữ liệu hoặc hoạt động chung (ví dụ: máy nhiễm virus thông thường, lỗi phần mềm đơn lẻ).

- Mức 2 (Trung bình): Sự cố ảnh hưởng đến một nhóm người dùng hoặc một dịch vụ nội bộ, có nguy cơ lây lan (ví dụ: mã độc lây qua LAN, sự cố Trang TTĐT).

- Mức 3 (Cao): Sự cố ảnh hưởng nghiêm trọng đến toàn bộ hệ thống, gây ngưng trệ hoạt động giải quyết TTHC, rò rỉ/mất mát/mã hóa dữ liệu (ví dụ: Tấn công Ransomware, tấn công từ chối dịch vụ (DDoS) vào hệ thống Một cửa, hệ thống chủ bị chiếm quyền).

- Mức 4 (Rất cao/Nghiêm trọng): Sự cố gây ảnh hưởng nghiêm trọng đến an ninh quốc gia, trật tự an toàn xã hội hoặc gây thiệt hại đặc biệt lớn về kinh tế.

III. NỘI DUNG THỰC HIỆN

1. Đánh giá các nguy cơ, sự cố ATTT mạng

a) Đánh giá hiện trạng và khả năng bảo đảm ATTT mạng của hệ thống thông tin và các đối tượng cần bảo vệ; đánh giá, dự báo các nguy cơ, sự cố, tấn công mạng có thể xảy ra với các hệ thống thông tin và các đối tượng cần bảo vệ; đánh giá, dự báo các hậu quả, thiệt hại, tác động nếu xảy ra sự cố; đánh giá về hiện trạng phương tiện, trang thiết bị, công cụ hỗ trợ, nhân lực, vật lực phục vụ đối phó, ứng cứu, khắc phục sự cố (bao gồm cả đơn vị cung cấp dịch vụ nếu có).

- Đơn vị chủ trì: Phòng Văn hóa – Xã hội, Trung tâm phục vụ Hành chính công;

- Đơn vị phối hợp: Công an phường; Tổ Ứng cứu Công nghệ và Nghiệp vụ hỗ trợ giải quyết TTHC; Tổ Công nghệ số cộng đồng phường; các doanh nghiệp cung cấp dịch vụ viễn thông, internet; doanh nghiệp cung cấp dịch vụ ATTT mạng (trường hợp thuê dịch vụ) và các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: Thường xuyên.

b) Chủ động thực hiện săn lùng mối nguy hại và rà quét lỗ hổng trên các hệ thống thông tin trong phạm vi quản lý; khắc phục các lỗ hổng, điểm yếu theo cảnh báo của cơ quan chức năng (thực hiện theo quy định tại Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ).

- Đơn vị chủ trì: Phòng Văn hóa - Xã hội, Trung tâm phục vụ Hành chính công.

- Đơn vị phối hợp: Công an phường; Tổ Ứng cứu Công nghệ và Nghiệp vụ hỗ trợ giải quyết TTHC; Tổ Công nghệ số cộng đồng phường; các doanh nghiệp cung cấp dịch vụ viễn thông, internet; doanh nghiệp cung cấp dịch vụ ATTT mạng (nếu có) và các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: Hàng năm (tối thiểu 01 lần/06 tháng).

2. Phương án đối phó, ứng cứu đối với một số tình huống sự cố cụ thể

Đối với mỗi hệ thống thông tin, chương trình ứng dụng, cần xây dựng tình huống, kịch bản sự cố cụ thể và đưa ra phương án đối phó, ứng cứu sự cố tương ứng. Trong phương án đối phó, ứng cứu phải đặt ra được các tiêu chí để có thể nhanh chóng xác định được tính chất, mức độ của sự cố khi sự cố xảy ra. Việc xây dựng phương án đối phó, ứng cứu sự cố và tuân thủ theo các quy định, hướng dẫn, bảo đảm các nội dung sau:

a) Quy trình triển khai và các bước ưu tiên ứng cứu ban đau khi hệ thống thông tin gặp sự cố, có phân theo các loại sự cố thực hiện theo mục c, Phần 3. Triển khai hoạt động thường trực, điều phối, xử lý, ứng cứu sự cố của Kế hoạch này.

b) Phương pháp, cách thức để xác định nhanh chóng, kịp thời nguyên nhân, nguồn gốc sự cố nhằm áp dụng phương án đối phó, ứng cứu, khắc phục sự cố phù hợp. Các sự cố thường gặp:

- Sự cố do bị tấn công mạng.

- Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc do lỗi đường điện, đường truyền, hosting...

- Sự cố do lỗi của người quản trị, vận hành hệ thống.

- Sự cố liên quan đến các thiên tai, thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn và các sự cố gây mất ATTT mạng khác.

c) Phương án đối phó, khắc phục sự cố đối với một hoặc nhiều tình huống.

- Tình huống sự cố do bị tấn công mạng:

+ Tấn công từ chối dịch vụ;

+ Tấn công giả mạo;

+ Tấn công sử dụng mã độc;

+ Tấn công truy cập trái phép, chiếm quyền điều khiển;

+ Tấn công thay đổi giao diện;

+ Tấn công mã hóa phần mềm, dữ liệu, thiết bị;

+ Tấn công phá hoại thông tin, dữ liệu, phần mềm;

+ Tấn công nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu;

+ Tấn công tổng hợp sử dụng kết hợp nhiều hình thức;

+ Các hình thức tấn công mạng khác.

- Tình huống sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật:

+ Sự cố nguồn điện;

+ Sự cố đường kết nối Internet;

+ Sự cố do lỗi phần mềm, phần cứng, ứng dụng của hệ thống thông tin;

+ Sự cố liên quan đến quá tải hệ thống;

+ Sự cố khác do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật.

- Tình huống sự cố do lỗi của người quản trị, vận hành hệ thống:

+ Lỗi trong cập nhật, thay đổi, cấu hình phần cứng;

+ Lỗi trong cập nhật, thay đổi, cấu hình phần mềm;

+ Lỗi liên quan đến chính sách và thủ tục ATTT;

+ Lỗi liên quan đến việc dừng dịch vụ vì lý do bắt buộc;

+ Lỗi khác liên quan đến người quản trị, vận hành hệ thống.

- Tình huống sự cố liên quan đến các thiên tai, thảm họa tự nhiên, như bão, lụt, động đất, hỏa hoạn và các sự cố gây mất ATTT mạng khác.

d) Công tác tổ chức, điều hành, phối hợp giữa các lực lượng trong đối phó, ngăn chặn, ứng cứu, khắc phục sự cố.

- Đơn vị chủ trì: Tổ Ứng cứu Công nghệ và Nghiệp vụ hỗ trợ giải quyết TTHC.

- Đơn vị phối hợp: Công an phường; Phòng Văn hóa - Xã hội; các ban, ngành, doanh nghiệp; Tổ công tác về phát triển khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số và Cải cách hành chính; các doanh nghiệp cung cấp dịch vụ viễn thông, internet; doanh nghiệp cung cấp dịch vụ ATTT mạng (nếu có); các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: Thường xuyên hàng năm.

đ) Phương án về nhân lực, trang thiết bị, phần mềm, phương tiện, công cụ, và dự kiến kinh phí để thực hiện, đối phó, ứng cứu, xử lý đối với từng tình huống sự cố cụ thể.

- Đơn vị chủ trì: Tổ Ứng cứu Công nghệ và Nghiệp vụ hỗ trợ giải quyết TTHC; Tổ Công nghệ số cộng đồng phường;

- Đơn vị phối hợp: các doanh nghiệp cung cấp dịch vụ viễn thông, internet; doanh nghiệp cung cấp dịch vụ ATTT mạng (nếu có); các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: Thường xuyên hàng năm.

3. Triển khai hoạt động thường trực, điều phối, xử lý, ứng cứu sự cố

a) Báo cáo sự cố ATTT mạng

- Đơn vị thực hiện: Đơn vị quản lý, vận hành hệ thống thông tin báo cáo cơ quan chủ quản hệ thống thông tin, Công an phường, Tổ Ứng cứu Công nghệ và Nghiệp vụ hỗ trợ giải quyết TTHC.

- Thời gian thực hiện: Ngay khi xảy ra sự cố và được duy trì trong suốt quá trình ứng cứu sự cố.

b) Tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố ATTT mạng

- Đơn vị chủ trì: Đơn vị quản lý, vận hành hệ thống thông tin (các cơ quan, đơn vị); Công an phường, Tổ Ứng cứu Công nghệ và Nghiệp vụ hỗ trợ giải quyết TTHC; Tổ Công nghệ số cộng đồng phường.

- Đơn vị phối hợp: Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam – VNCERT, Đội ứng cứu sự cố An toàn thông tin mạng tỉnh Gia Lai; tổ chức, cá nhân gửi thông báo, báo cáo sự cố; các doanh nghiệp cung cấp dịch vụ

viễn thông, internet; doanh nghiệp cung cấp dịch vụ ATTT mạng (nếu có); các cơ quan, đơn vị chức năng liên quan.

- Thời gian thực hiện: Ngay sau khi phát hiện sự cố hoặc nhận được thông báo, báo cáo sự cố của tổ chức, cá nhân.

c) Quy trình ứng cứu sự cố ATTT mạng thông thường và nghiêm trọng theo quy định tại Điều 13 và Điều 14 Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ và Điều 11 Thông tư 20/2017/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông

- Đơn vị chủ trì: Đơn vị vận hành hệ thống thông tin; Tổ Ứng cứu Công nghệ và Nghiệp vụ hỗ trợ giải quyết TTHC; Công an phường;

- Đơn vị phối hợp: Các ban, ngành, doanh nghiệp nhà nước; Tổ Công nghệ số cộng đồng phường; Đội UCSC ATTTM tỉnh Gia Lai.

- Thời gian thực hiện: Triển khai ngay sau khi tiếp nhận thông báo sự cố; cập nhập quy trình hàng năm hoặc khi có sự thay đổi.

4. Triển khai huấn luyện, diễn tập, phòng ngừa sự cố, giám sát phát hiện, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố

Xây dựng các nội dung, nhiệm vụ cụ thể cần triển khai nhằm phòng ngừa sự cố, giám sát phát hiện, huấn luyện, diễn tập, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố. Đồng thời cần đáp ứng đúng theo quy định tại Chỉ thị số 60/CT-BTTTT ngày 16/9/2021 của Bộ Thông tin và Truyền thông về việc tổ chức triển khai diễn tập thực chiến bảo đảm an toàn thông tin mạng, bao gồm:

a) Triển khai các chương trình huấn luyện, diễn tập.

- Tổ chức diễn tập các phương án đối phó, ứng cứu sự cố tương ứng với các kịch bản, tình huống sự cố cụ thể; huấn luyện, diễn tập nâng cao kỹ năng, nghiệp vụ phối hợp, ứng cứu, chống tấn công, xử lý mã độc, khắc phục sự cố; tham gia huấn luyện, diễn tập vùng, miền, quốc gia, quốc tế.

- Đơn vị chủ trì: Tổ Ứng cứu Công nghệ và Nghiệp vụ hỗ trợ giải quyết TTHC, Công an phường.

- Đơn vị phối hợp: Đơn vị quản lý, vận hành hệ thống thông tin; Đội UCSC ATTTM tỉnh Gia Lai, Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT; các doanh nghiệp cung cấp dịch vụ viễn thông, internet; doanh nghiệp cung cấp dịch vụ ATTT (nếu có); các cơ quan, đơn vị chức năng có liên quan.

- Thời gian thực hiện: Hàng năm.

b) Triển khai nhiệm vụ nhằm phòng ngừa sự cố và phát hiện sớm sự cố.

- Thực hiện nghiêm công tác giám sát, phát hiện sớm 7 nguy cơ, sự cố; phòng ngừa sự cố, quản lý rủi ro; nghiên cứu, phân tích, xác minh, cảnh báo sự cố, rủi ro an toàn thông tin mạng, phần mềm độc hại; xây dựng, áp dụng quy

trình, quy định, tiêu chuẩn an toàn thông tin; tuyên truyền, nâng cao nhận thức về nguy cơ, sự cố, tấn công mạng.

- Đơn vị chủ trì: Tổ Ứng cứu Công nghệ và Nghiệp vụ hỗ trợ giải quyết TTHC, Công an phường; đơn vị quản lý, vận hành hệ thống thông tin; Tổ Công nghệ số cộng đồng phường.

- Đơn vị phối hợp: Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT; Đội UCSC ATTTM tỉnh Gia Lai, các sở, ban, ngành, doanh nghiệp nhà nước; UBND tỉnh; các cơ quan, đơn vị chức năng có liên quan.

- Thời gian thực hiện: Thường xuyên, hàng năm.

c) Các nội dung, nhiệm vụ nhằm bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố.

- Mua sắm, nâng cấp, gia hạn bản quyền trang thiết bị, phần mềm, công cụ, phương tiện phục vụ ứng cứu, khắc phục sự cố; chuẩn bị các điều kiện bảo đảm, dự phòng nhân lực, vật lực, tài chính để sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố xảy ra; tổ chức hoạt động của Đội ứng cứu sự cố, bộ phận ứng cứu sự cố; thuê dịch vụ kỹ thuật và tổ chức, duy trì đội chuyên gia ứng cứu sự cố; tổ chức và tham gia các hoạt động của mạng lưới ứng cứu sự cố.

- Đơn vị chủ trì: Tổ Ứng cứu Công nghệ và Nghiệp vụ hỗ trợ giải quyết TTHC, Công an phường; các ban, ngành, doanh nghiệp nhà nước trên địa bàn phường.

- Đơn vị phối hợp: Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT; Đội UCSC ATTTM tỉnh Gia Lai, các cơ quan, đơn vị chức năng có liên quan.

- Thời gian thực hiện: Hàng năm.

IV. TỔ CHỨC LỰC LƯỢNG ỨNG PHÓ SỰ CỐ

1. Ban Chỉ đạo (BCĐ) ứng phó sự cố ATTT phường:

1.1. Thành phần:

- Trưởng ban: Chủ tịch UBND phường;

- Phó Trưởng ban: Phó Chủ tịch UBND phường – phụ trách VHXH;

- Thành viên thường trực (Kỹ thuật): Công chức phụ trách ATTT;

- Thành viên (Nghiệp vụ): Tổ Ứng cứu Công nghệ và Hỗ trợ giải quyết TTHC, Công an phường.

- Thành viên: Công chức Tư pháp - Hộ tịch, Địa chính - Xây dựng.

1.2 Chức năng: Chỉ đạo, điều hành toàn diện công tác ứng cứu. Quyết định phương án xử lý, huy động nguồn lực, và là đầu mối phát ngôn chính thức với bên ngoài.

2. Công chức phụ trách ATTT

2.1. Vai trò: Lực lượng thường trực, nòng cốt kỹ thuật tại chỗ. Là đầu mối kỹ thuật của phường.

2.2. Nhiệm vụ:

2.2.1. Trước sự cố (Chuẩn bị):

- Thường xuyên giám sát, vận hành các hệ thống kỹ thuật (Firewall, Antivirus).

- Chủ động rà quét lỗ hổng, cập nhật bản vá cho máy chủ, máy trạm, Trang TTĐT.

- Quản lý và thực hiện sao lưu (backup) dữ liệu định kỳ.

- Duy trì danh bạ liên lạc khẩn cấp (Lãnh đạo, Gia Lai CERT, ISPs, Vendor phần mềm).

2.2.2. Trong sự cố (Ứng phó):

- Là người đầu tiên tiếp nhận thông tin sự cố (từ CBCC, người dân...).

- Thực hiện phân loại ban đầu (Mức 1, 2, 3) và báo cáo ngay Trưởng BCĐ.

- Thực hiện các hành động ngăn chặn ban đầu (ví dụ: cô lập máy tính/vùng mạng bị nhiễm, ngắt kết nối Internet, tạm dừng dịch vụ).

- Chủ trì, phối hợp với các bên (nội bộ và bên ngoài) để phân tích, tìm nguyên nhân.

- Trực tiếp liên lạc, báo cáo, yêu cầu hỗ trợ từ Gia Lai CERT đối với sự cố Mức 2, 3.

2.2.3. Sau sự cố (Khôi phục):

- Chủ trì thực hiện khôi phục hệ thống (cài đặt lại, phục hồi dữ liệu từ backup).

- Rà soát, khắc phục triệt để lỗ hổng (patching) đã bị khai thác.

- Lập biên bản, báo cáo tổng kết, rút kinh nghiệm về sự cố.

3. Tổ Ứng cứu Công nghệ và Nghiệp vụ hỗ trợ giải quyết TTHC (Tổ TTHC):

3.1. Vai trò: Lực lượng đảm bảo tính liên tục của hoạt động nghiệp vụ, đặc biệt là giải quyết TTHC.

3.2. Chức năng: Tập trung vào "Nghiệp vụ" và "Con người" khi "Công nghệ" gặp sự cố.

3.3. Nhiệm vụ:

3.3.1. Trước sự cố (Chuẩn bị):

- Xây dựng và diễn tập Quy trình giải quyết TTHC thủ công/dự phòng (sử dụng biểu mẫu giấy, sổ theo dõi...) khi hệ thống Một cửa điện tử lỗi.

- Đảm bảo các biểu mẫu, sổ sách dự phòng luôn sẵn sàng.

3.3.2. Trong sự cố (Ứng phó):

- Ngay khi nhận thông báo sự cố (từ Công chức ATTT hoặc Trưởng BCĐ), lập tức kích hoạt quy trình dự phòng.

- Trực tiếp thông báo, hướng dẫn, giải thích rõ ràng cho công dân, tổ chức tại Bộ phận Một cửa về sự cố và phương án giải quyết tạm thời (tránh gây hoang mang, bức xúc).

- Ghi nhận hồ sơ thủ công, hẹn ngày trả kết quả (có dự trù thêm thời gian khắc phục).

3.3.3. Sau sự cố (Khôi phục):

- Phối hợp với Công chức ATTT để kiểm tra, xác thực (validate) dữ liệu trên hệ thống sau khi được khôi phục.

- Thực hiện nhập (hồi) lại dữ liệu từ các hồ sơ giấy đã tiếp nhận trong thời gian sự cố vào hệ thống Một cửa điện tử, đảm bảo tính liên thông và đồng bộ.

4. Đội ứng cứu sự cố ATTT mạng tỉnh Gia Lai (Gia Lai CERT):

4.1. Vai trò: Lực lượng hỗ trợ chuyên sâu cấp tỉnh.

4.2. Chức năng: Điều phối, hỗ trợ kỹ thuật chuyên sâu (forensics, phân tích mã độc, gỡ bỏ) khi sự cố vượt quá khả năng xử lý tại chỗ của phường.

4.3. Nhiệm vụ (khi nhận được yêu cầu từ phường):

- Tiếp nhận, xác minh thông tin sự cố.

- Cung cấp hướng dẫn, tư vấn kỹ thuật từ xa (qua điện thoại, email, kênh bảo mật).

- Cử cán bộ chuyên gia xuống hỗ trợ trực tiếp tại phường (nếu là sự cố Mức 3 hoặc theo chỉ đạo của UBND tỉnh).

- Phối hợp với các đơn vị cấp quốc gia (VNCERT/CC, A05-Bộ Công an) nếu sự cố có quy mô lớn.

V. QUY TRÌNH PHỐI HỢP ỨNG CỨU TỔNG QUÁT (05 GIAI ĐOẠN)

1. Giai đoạn 1: Chuẩn bị

- Công chức ATTT: Định kỳ (hàng quý) rà quét, vá lỗi; (hàng tuần) sao lưu dữ liệu quan trọng; (thường xuyên) cập nhật phần mềm Antivirus.

- Tổ TTHC: (Hàng quý) kiểm tra lại các biểu mẫu, sổ sách dự phòng.

- BCĐ: (Hàng năm) tổ chức diễn tập, tập huấn nội bộ.

2. Giai đoạn 2: Phát hiện và Báo cáo

- Người phát hiện (CBCC, Tổ TTHC): Ngay lập tức báo cáo cho Công chức phụ trách ATTT (qua điện thoại/trực tiếp).

- Công chức ATTT: Xác minh, phân loại sự cố (Mức 1, 2, 3) trong vòng 15 phút.

- Công chức ATTT: Báo cáo ngay Trưởng BCĐ (Lãnh đạo UBND) về tình hình và mức độ.

- Trưởng BCĐ:

+ Nếu Mức 1: Giao Công chức ATTT tự xử lý.

+ Nếu Mức 2: Chỉ đạo Công chức ATTT xử lý, Tổ TTHC chuẩn bị phương án dự phòng.

+ Nếu Mức 3: Kích hoạt toàn bộ Kế hoạch. Chỉ đạo Công chức ATTT báo cáo khẩn cấp cho Gia Lai CERT (qua Hotline/Email).

3. Giai đoạn 3: Ngăn chặn và Phân tích

- Công chức ATTT: Thực hiện ngăn chặn kỹ thuật:

- Sự cố máy trạm (Malware): Ngắt cáp mạng/Wifi của máy bị nhiễm.

- Sự cố hệ thống (Ransomware, Deface): Tạm ngắt kết nối Internet của máy chủ, hoặc tạm dừng Trang TTĐT/Phần mềm.

- Tổ TTHC: (Nếu sự cố ảnh hưởng Một cửa) Kích hoạt quy trình thủ công, thông báo cho công dân.

- Gia Lai CERT: (Nếu được báo cáo) Hướng dẫn từ xa, yêu cầu cung cấp log, mẫu mã độc; bắt đầu phân tích.

4. Giai đoạn 4: Khắc phục và Phục hồi

- Công chức ATTT: (Dưới sự hướng dẫn của Gia Lai CERT nếu là Mức 3)

+ Tìm và loại bỏ triệt để nguyên nhân (mã độc, lỗ hổng).

+ Khôi phục dữ liệu từ bản sao lưu sạch gần nhất.

+ Cài đặt lại hệ thống (nếu cần).

+ Kiểm tra, vá tất cả các lỗ hổng liên quan.

- Gia Lai CERT: Cung cấp file diệt mã độc (nếu có), hướng dẫn vá lỗi, xác nhận hệ thống đã sạch.

- Tổ TTHC: (Sau khi Công chức ATTT xác nhận hệ thống ổn định)

+ Kiểm tra, đối chiếu tính toàn vẹn của dữ liệu nghiệp vụ (hồ sơ TTHC).

+ Tiến hành nhập lại dữ liệu hồ sơ thủ công vào hệ thống.

+ Báo cáo Trưởng BCĐ về việc sẵn sàng tiếp nhận hồ sơ trực tuyến trở lại.

5. Giai đoạn 5: Hoạt động sau sự cố

- Trưởng BCĐ: Chỉ đạo đưa hệ thống vào hoạt động bình thường, quyết định thời điểm công bố kết thúc sự cố.

- Công chức ATTT: Lập báo cáo tổng kết sự cố (nguyên nhân, thiệt hại, quá trình xử lý, bài học kinh nghiệm).

- BCĐ: Họp rút kinh nghiệm, cập nhật lại Kế hoạch/Quy trình (nếu cần).

VI. KỊCH BẢN ỨNG PHÓ MỘT SỐ TÌNH HUỐNG CỤ THỂ

1. Kịch bản 1: Hệ thống Một cửa điện tử bị ngưng trệ (do lỗi phần mềm, mất kết nối máy chủ)

1.1. Phát hiện: Tổ TTHC phát hiện không thể truy cập, báo Công chức ATTT.

1.2. Phân loại: Mức 2 hoặc 3 (nếu kéo dài).

1.3. Ứng phó

1.3.1. Nghiệp vụ (Tổ TTHC):

- Kích hoạt ngay quy trình dự phòng (tiếp nhận hồ sơ giấy).

- Thông báo, hướng dẫn công dân tại quầy.

1.3.2. Kỹ thuật (Công chức ATTT):

- Kiểm tra kết nối mạng nội bộ, kết nối Internet.

- Liên hệ ngay nhà cung cấp phần mềm (Vendor) và Gia Lai CERT (nếu cần) để báo lỗi và yêu cầu hỗ trợ.

- Phối hợp với Vendor để khởi động lại dịch vụ, kiểm tra cơ sở dữ liệu.

1.4. Phục hồi (Tổ TTHC): Sau khi hệ thống hoạt động, nhập lại hồ sơ giấy và kiểm tra dữ liệu.

2. Kịch bản 2: Tấn công Mã độc tống tiền (Ransomware) vào máy chủ hoặc máy trạm quan trọng

1.1. Phát hiện: CBCC thấy file bị mã hóa, báo Công chức ATTT.

1.2. Phân loại: Mức 3 (Nghiêm trọng).

1.3. Ứng phó:

1.3.1. Công chức ATTT:

- Lập tức ngắt kết nối mạng của máy bị nhiễm.

- KHÔNG trả tiền chuộc.

- Báo cáo ngay Trưởng BCĐ.

1.3.2. Trưởng BCĐ: Chỉ đạo Công chức ATTT báo cáo khẩn cấp Gia Lai CERT.

1.3.3. Công chức ATTT: (Theo hướng dẫn của Gia Lai CERT)

- Cô lập toàn bộ vùng mạng liên quan.

- Sử dụng Antivirus (đã cập nhật) quét toàn bộ hệ thống.

- Cài đặt lại hoàn toàn máy bị nhiễm.

- Khôi phục dữ liệu từ bản sao lưu sạch (offline) gần nhất.

3. Kịch bản 3: Tấn công Thay đổi giao diện (Deface) Trang TTĐT của phường

3.1. Phát hiện: Công chức ATTT (qua giám sát) hoặc người dân/CBCC báo.

3.2. Phân loại: Mức 2 hoặc 3 (tùy nội dung bị thay đổi).

3.3. Ứng phó:

Công chức ATTT thực hiện các nhiệm vụ sau:

- Lập tức ngắt kết nối Trang TTĐT khỏi Internet (chuyển sang chế độ bảo trì).

- Báo cáo Trưởng BCĐ và Gia Lai CERT.

- Thực hiện theo hướng dẫn của Gia Lai CERT.

- Rà soát log, tìm lỗ hổng (SQL Injection, Lỗi upload file...)

- Khôi phục lại giao diện và nội dung từ bản sao lưu sạch gần nhất.

- Bắt buộc vá lỗ hổng bảo mật trước khi đưa Trang TTĐT hoạt động trở lại.

4. Kịch bản 4: Tấn công Từ chối dịch vụ (DDoS) vào Trang TTĐT hoặc Dịch vụ công

4.1. Phát hiện: Hệ thống truy cập rất chậm hoặc không thể truy cập, báo Công chức ATTT.

4.2. Phân loại: Mức 3.

4.3. Ứng phó:

Công chức ATTT thực hiện các nhiệm vụ sau

- Kiểm tra băng thông, xác định dấu hiệu DDoS (lượng truy cập bất thường).

- Báo cáo Trưởng BCĐ.

- Liên hệ Gia Lai CERT và Nhà cung cấp dịch vụ Internet (ISP - VNPT/Viettel...) để yêu cầu hỗ trợ ngăn chặn (lọc IP, chặn luồng tấn công).

- Phục hồi: Hệ thống tự phục hồi sau khi ISP và Gia Lai CERT chặn đứng cuộc tấn công.

VII. KINH PHÍ THỰC HIỆN

Nguồn kinh phí thực hiện Kế hoạch được bố trí từ nguồn ngân sách nhà nước theo phân cấp ngân sách hiện hành; lồng ghép với kinh phí thực hiện các chương trình, kế hoạch, đề án khác có liên quan và các nguồn kinh phí hợp pháp khác theo quy định của pháp luật.

VIII. TỔ CHỨC THỰC HIỆN

1. Các cơ quan, đơn vị, doanh nghiệp trên địa bàn phường.

- Phòng Văn hóa – Xã hội là cơ quan thường trực, phối hợp Trung tâm phục vụ Hành chính công, Văn phòng HĐND và UBND tham mưu, triển khai, đôn đốc và tổng hợp báo cáo thực hiện Kế hoạch này.

- Xây dựng nội dung, lập dự toán kinh phí thực hiện các nhiệm vụ về ứng phó sự cố, bảo đảm ATTT mạng của cơ quan, đơn vị, kinh phí hoạt động cho Tổ Ứng cứu Công nghệ và Nghiệp vụ hỗ trợ giải quyết TTHC.

- Định kỳ 06 tháng và hàng năm, hoặc đột xuất báo cáo tình hình ứng phó sự cố, bảo đảm ATTT mạng tại các Phòng ban, ngành, công an phường báo cáo UBND phường để tổng hợp báo cáo các cơ quan cấp trên theo quy định.

- Cử cán bộ tham gia các chương trình huấn luyện, diễn tập và khóa đào tạo, tập huấn về ứng cứu sự cố, bảo đảm ATTT mạng để nâng cao kỹ năng và công tác tham mưu, triển khai giám sát, bảo đảm ATTT mạng.

- Thực hiện đánh giá, xác định cấp độ, lập hồ sơ đề xuất cấp độ an toàn 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 thông tin theo cấp độ và Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông quy định chi tiết một số điều của Nghị định số 85/2016/NĐ-CP.

- Tổ chức tuyên truyền, phổ biến các văn bản quy phạm pháp luật, tài liệu hướng dẫn chuyên môn, các hoạt động liên quan đến bảo đảm ATTT mạng của phường, của cơ quan đơn vị trên Trang thông tin điện tử, các phương tiện thông tin đại chúng.

2. Công an phường

- Tổ chức theo dõi, đôn đốc, phối hợp với các ban, ngành trong việc triển khai thực hiện Kế hoạch. Định kỳ 06 tháng, hàng năm hoặc đột xuất tổng hợp báo cáo kết quả thực hiện gửi UBND phường để theo dõi, chỉ đạo.

- Tham mưu, tổ chức thực thi, đôn đốc, kiểm tra, đánh giá, giám sát, hướng dẫn công tác bảo đảm ATTT định kỳ hàng năm hoặc theo chỉ đạo của UBND phường đối với các cơ quan nhà nước, doanh nghiệp trên địa bàn phường. Tiến hành xử lý theo quy định của pháp luật các cá nhân, cơ quan vi phạm trong công tác bảo đảm ATTT mạng.

3. Phòng Văn hóa - Xã hội

- Tổ chức triển khai, xây dựng, quản lý, vận hành hạ tầng mạng, hạ tầng, nền tảng, cơ sở dữ liệu dùng chung, phục vụ chuyển đổi số, ứng dụng công nghệ thông tin; phối hợp Công an phường trong thực hiện công tác bảo đảm an toàn thông tin đối với hệ thống thông tin tập trung, dùng chung của phường.

- Cử cán bộ có trình độ, kinh nghiệm tham gia xử lý, ứng cứu các sự cố về an toàn thông tin, an ninh mạng xảy ra trên địa bàn phường khi có yêu cầu của đơn vị điều phối.

- Tiếp tục bảo đảm an toàn thông tin, trao đổi kịp thời cho Công an phường mọi thông tin liên quan đến các sự cố gây mất an ninh mạng, an toàn thông tin đối với hệ thống thông tin tập trung, dùng chung của phường.

- Phối hợp Công an phường phát huy thế mạnh về truyền thông phục vụ triển khai hiệu quả công tác tuyên truyền, phổ biến pháp luật về an toàn thông tin, an ninh mạng.

4. Phòng Kinh tế - Hạ tầng – Đô thị

Căn cứ khả năng cân đối ngân sách phường, tham mưu cho cấp có thẩm quyền bố trí kinh phí thực hiện Kế hoạch này theo quy định.

5. Tổ Ứng cứu Công nghệ và Nghiệp vụ giải quyết TTHC:

- Là đầu mối đảm bảo ATTT tại đơn vị.

- Chịu trách nhiệm xây dựng, hoàn thiện và tổ chức diễn tập quy trình nghiệp vụ dự phòng; đảm bảo sẵn sàng biểu mẫu, sổ sách.

6. Cán bộ, công chức, viên chức và người lao động UBND phường: Có trách nhiệm tuân thủ các quy định về ATTT, tham gia đầy đủ các buổi tập huấn, diễn tập và báo cáo sự cố kịp thời.

Trên đây là Kế hoạch Ứng phó sự cố, bảo đảm ATTT mạng trên địa bàn phường Hoài Nhơn Nam. Đề nghị các cơ quan, đơn vị nghiêm túc triển khai thực hiện. Trong quá trình thực hiện nếu phát sinh khó khăn, vướng mắc, các cơ quan, đơn vị phản ánh, kiến nghị về Phòng Văn hóa – Xã hội để tổng hợp, báo cáo UBND phường xem xét, quyết định./

Nơi nhận:
- Công an tỉnh Gia Lai;
- Sở Khoa học và Công nghệ;
- Chủ tịch, các PCT UBND phường;
- Các cơ quan, ban, ngành, đoàn thể phường;
- Lưu: VT.

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

U.B.N.D PHƯỜNG HOÀI NHƠN NAM T. GIA LAI

Trần Chí Trung