ỦY BAN NHÂN DÂN XÃ NGỌC LIÊN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 39 /KH-UBND	*Ngọc Liên, ngày 27 tháng 02 năm 2026*

KẾ HOẠCH
Ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn xã Ngọc Liên

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 Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) 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 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ về ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Quyết định số 1622/QĐ-TTg ngày 25/10/2017 của Thủ tướng Chính phủ phê duyệt Đề án Đẩy mạnh hoạt động của mạng lưới ứng cứu sự cố, tăng cường năng lực cho các cán bộ, bộ phận chuyên trách ứng cứu sự cố an toàn thông tin mạng trên toàn quốc đến 2020, định hướng đến 2025;

Căn cứ Quyết định số 1017/QĐ-TTg ngày 14/8/2018 của Thủ tướng Chính phủ phê duyệt Đề án giám sát an toàn thông tin mạng đối với hệ thống, dịch vụ công nghệ thông tin phục vụ Chính phủ đến năm 2020, định hướng đến năm 2025;

Căn cứ Quyết định số 964/QĐ-TTg ngày 10/8/2022 của Thủ tướng Chính phủ phê duyệt chiến lược an toàn, an ninh mạng quốc gia, chủ động ứng phó với các thách thức không gian mạng đến năm 2025, tầm nhìn 2030;

Căn cứ Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng chống phần mềm độc hại; Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam;

Căn cứ Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam;

Căn cứ Chỉ thị số 09/CT-TTg ngày 23/02/2024 của Thủ tướng Chính phủ về tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ; Căn cứ Chỉ thị số 60/CT-BTTTT ngày 16/9/2021 của Bộ Thông tin và

Truyền thông (nay là Bộ Khoa học và Công nghệ) về việc tổ chức triển khai diễn tập thực chiến bảo đảm an toàn thông tin mạng;

Ủy ban nhân dân xã Ngọc Liên ban hành kế hoạch Ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn xã Ngọc Liên như sau.

I. MỤC ĐÍCH, YÊU CẦU VÀ QUY ĐỊNH CHUNG.

1. Mục đích.

- Bảo đảm an toàn thông tin cho các hệ thống thông tin quan trọng trên địa bàn xã; 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.

- Tạo chuyển biến mạnh mẽ trong nhận thức về an toàn thông tin mạng đối với cán bộ, công chức, viên chức trong các cơ quan nhà nước của xã.

- Xây dựng, phát triển Đội ứng cứu sự cố an toàn thông tin mạng xã 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.

- 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.

2. Yêu cầu.

- Các hệ thống thông tin của các phòng ban, ngành của xã 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.

- Hoạt động ứng cứu sự cố ATTT mạng phải chuyển từ bị động sang chủ động, bao gồm: 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.

- Xác định cụ thể các nguồn lực, giải pháp tổ chức thực hiện và kinh phí để triển khai các nội dung của Kế hoạch, bảo đảm khả thi, hiệu quả.

- 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 xã; 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).

3. Quy định chung.

3.1. Phạm vi và đối tượng.

Kế hoạch này để ứng phó sự cố, bảo đảm an toàn thông tin mạng đối với các hệ thống thông tin của xã, 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 xã.

3.2. Nguyên tắc, phương châm ứng phó sự cố.

- 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.

3.3. Các lực lượng tham gia ứng phó sự cố.

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

- Tổ ứng cứu sự cố ATTT mạng của xã (lực lượng chính ứng phó sự cố, trong đó Công an xã là cơ quan thường trực).

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

- 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.

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

- Công an xã Ngọc Liên: Đơn vị chuyên trách ứng cứu sự cố ATTT mạng của xã; thực hiện chỉ đạo, tổ chức triển khai hoạt động ứng phó sự cố ATTT mạng và các nhiệm vụ khác khi xảy ra sự cố.

- Tổ ứng cứu sự cố ATTT mạng của xã: 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 khi có yêu cầu từ Công an xã hoặc các cơ quan có liên quan.

- Chịu trách nhiệm 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 xã; xử lý, ứng cứu các sự cố về an toàn thông tin, an ninh mạng xảy ra trên địa bàn xã khi có yêu cầu của đơn vị điều phối.

- 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 xã (Công an xã) trong công tác ứng phó, xử lý các sự cố.

- Doanh nghiệp cung cấp, xây dựng các hệ thống thông tin: Phối hợp với Công an xã, 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 Công an xã, 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.

II. NỘI DUNG THỰC HIỆN.

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

1.1. Đánh giá hiện trạng và nguy cơ.

- 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: Văn phòng HĐND và UBND xã.

- Đơn vị phối hợp: Công an xã; Tổ ứng cứu sự cố ATTT mạng của xã; 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.

1.2. Chủ động rà quét, săn lùng mối nguy.

- 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: Văn phòng HĐND và UBND xã.

- Đơn vị phối hợp: Công an xã; Tổ ứng cứu sự cố ATTT mạng của xã; 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:

2.1. Quy trình triển khai và các bước ưu tiên ứng cứu ban đầu khi hệ thống thông tin gặp sự cố, có phân theo các loại sự cố thực hiện theo mục 3.3, Phần 3. Triển khai hoạt động thường trực, điều phối, xử lý, ứng cứu sự cố của Kế hoạch này.

2.2. 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.

2.3. 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.

2.4. 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: Tiểu ban an toàn, an ninh mạng xã Ngọc Liên.

- Đơn vị phối hợp: Công an xã; Văn phòng HĐND và UBND xã; các ban, ngành, doanh nghiệp; Tổ ứng cứu sự cố ATTT mạng của xã; 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.

2.5. 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: Công an xã, các ban, ngành, doanh nghiệp trên địa bàn xã.

- Đơn vị phối hợp: Tổ ứng cứu sự cố ATTT mạng của xã; 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.

3.1. 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 xã, Tổ ứng cứu sự cố ATTT mạng của xã.

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

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

- Đơn vị chủ trì: Công an xã; Đơn vị quản lý, vận hành hệ thống thông tin (các cơ quan, đơn vị); Tổ ứng cứu sự cố ATTT mạng của xã;

- Đơn vị phối hợp: Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT; 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.

3.3. 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; Công an xã;

- Đơn vị phối hợp: Các ban, ngành, doanh nghiệp nhà nước;

- Thời gian thực hiện: Triển khai ngay sau khi tiếp nhận thông báo sự cố; cập nhật 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:

4.1. Triển khai các chương trình huấn luyện, diễn tập.

- Nội dung thực hiện: 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: Công an xã; Đội ứng cứu sự cố ATTT của xã.

- Đơn vị phối hợp: Đơn vị quản lý, vận hành hệ thống thông tin; 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.

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

- Nội dung thực hiện: Thực hiện nghiêm công tác giám sát, phát hiện sớm 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: Công an xã; đơn vị quản lý, vận hành hệ thống thông tin; Tổ ứng cứu sự cố ATTT mạng của xã;

- Đơn vị phối hợp: Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT; 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.

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

- Nội dung thực hiện: 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: Công an xã; các ban, ngành, doanh nghiệp nhà nước trên địa bàn xã.

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

- Thời gian thực hiện: Hàng năm.

III. 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.

IV. TỔ CHỨC THỰC HIỆN.

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

- Văn phòng HĐND và UBND xã là đầu mối chịu trách nhiệm về ATTT mạng tại cơ quan, đơn vị theo thẩm quyền quản lý.

- Giao chuyên viên Văn phòng HĐND và UBND phụ trách công nghệ thông tin nhiệm vụ về ATTT mạng tại cơ quan, đơn vị.

- 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.

- 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 xã báo cáo UBND xã 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 xã, của cơ quan đơn vị trên Trang thông tin điện tử, các phương tiện thông tin đại chúng.

2. Công an xã.

- Là cơ quan đầu mối, chuyên trách về ứng cứu sự cố an toàn thông tin mạng trên địa bàn xã, có trách nhiệm xây dựng và triển khai Kế hoạch này; 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 xã để theo dõi, chỉ đạo.

- Tham mưu UBND xã ban hành quyết định kiện toàn Tổ ứng cứu sự cố ATTT mạng cho phù hợp với tình hình bảo đảm ATTT trên địa bàn xã Ngọc Liên khi có sự thay đổi.

- 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 xã đối với các cơ quan nhà nước, doanh nghiệp trên địa bàn xã. Tiến hành xử lý theo quy định của pháp luật các cá nhân, cơ quan vi phạm trong công tác bảo đảm ATTT mạng.

- Xây dựng nội dung, lập dự toán kinh phí bảo đảm cho hoạt động của Đơn vị chuyên trách ứng cứu sự cố và Tổ ứng cứu sự cố ATTT mạng của xã.

3. Văn phòng HĐND và UBND xã.

- 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 xã trong thực hiện công tác bảo đảm an toàn thông tin đối với hệ thống thông tin tập trung, dùng chung của xã Ngọc Liên.

- 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 xã Ngọc Liên khi có yêu cầu của đơn vị điều phối.

- Tiếp tục bảo đảm an toàn thông tin, trao đổi kịp thời cho Công an xã 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 xã.

4. Phòng Văn hóa - xã hội.

Phối hợp Công an xã 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.

5. Phòng Kinh tế.

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

Trên đây là Kế hoạch Ứng phó sự cố, bảo đảm ATTT mạng trên địa bàn xã Ngọc Liên. UBND xã 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 Công an xã (qua Tổ An ninh - phòng, chống tội phạm) để tổng hợp, báo cáo UBND xã xem xét, quyết định./.

Nơi nhận:
- Thường trực Đảng ủy (để b/c);
- Lãnh đạo UBND xã;
- Các phòng, ban chuyên môn;
- Công an xã;
- Trang thông tin điện tử xã;
- Lưu: VT, VHXH

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

U.B.N.D XÃ NGỌC LIÊN T.THANH HÓA

Phạm Xuân Khánh

PHỤ LỤC
DANH MỤC MẪU BIỂU
(Ban hành kèm theo Kế hoạch số /KH-UBND ngày tháng 02 năm 2026 của Ủy ban nhân dân xã Ngọc Liên)

STT	Mẫu số	Tên Mẫu biểu
1	Mầu số 01	Báo cáo ban đầu sự cố an toàn thông tin mạng
2	Mầu số 02	Báo cáo kết thúc ứng phó sự cố

ỦY BAN NHÂN DÂN XÃ NGỌC LIÊN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: /BC-UBND	*Ngọc Liên, ngày ... tháng ... năm ...*

BÁO CÁO BAN ĐẦU SỰ CỐ AN TOÀN THÔNG TIN MẠNG

I. THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN BÁO CÁO SỰ CỐ

- Tên tổ chức/cá nhân báo cáo sự cố (*) ……
- Địa chỉ: (*)……
- Điện thoại (*)……Email (*)……

NGƯỜI LIÊN HỆ

- Họ và tên (*) ……Chức vụ: ……
- Điện thoại (*) ……Email (*)……

II. THÔNG TIN CHI TIẾT VỀ HỆ THỐNG BỊ SỰ CỐ

Tên đơn vị vận hành hệ thống thông tin (*):	*Điền tên đơn vị vận hành hoặc được thuê vận hành hệ thống thông tin*
Cơ quan quản lý cấp trên:	*Điền tên cơ quan quản lý cấp trên*
Tên hệ thống bị sự cố	*Điền tên hệ thống bị sự cố và tên miền, địa chỉ IP liên quan*
Phân loại cấp độ của hệ thống thông tin, (nếu có)	□ Cấp độ 1 □ Cấp độ 2 □ Cấp độ 3 □ Cấp độ 4 □ Cấp độ 5
Tổ chức cung cấp dịch vụ an toàn thông tin mạng (nếu có):	*Điền tên nhà cung cấp ở đây*
Tên nhà cung cấp dịch vụ kết nối bên ngoài (nếu có)	*Điền tên nhà cung cấp ở đây*
Dải địa chỉ Public IP kết nối với hệ thống bên ngoài:	*Điền thông tin ở đây*
Mô tả sơ bộ về sự cố (*)	
Đề nghị cung cấp một bản tóm tắt ngắn gọn về sự cố, bao gồm đánh giá sơ bộ cuộc tấn công đã xảy ra chưa và bất kỳ các nguy cơ dẫn đến khả năng phá hoại hoặc gián đoạn dịch vụ. Xác định mức độ nhạy cảm của thông tin liên quan hoặc những đối tượng bị ảnh hưởng bởi sự cố:	

Ngày phát hiện sự cố (*) .... (dd/mm/yy)	Thời điểm phát hiện (*):	….giờ.. phút

HIỆN TRẠNG SỰ CỐ (*)

□ Đã được xử lý

□ Chưa được xử lý

CÁCH THỨC PHÁT HIỆN * *(Đánh dấu những cách thức được sử dụng để phát hiện sự cố).*

□ Qua hệ thống phát hiện xâm nhập
□ Kiểm tra dữ liệu lưu lại (Log File)
□ Nhận được thông báo từ:……
□ Khác, đó là ……

ĐÃ GỬI THÔNG BÁO SỰ CỐ CHO *

□ Công an tỉnh
□ ISP đang trực tiếp cung cấp dịch vụ
□ Các cơ quan chuyên trách an toàn thông tin mạng khác:

III. THÔNG TIN BỔ SUNG VỀ HỆ THỐNG XẢY RA Sự CỐ

• Hệ điều hành: ……Version:……
• Các dịch vụ có trên hệ thống *(Đánh dấu những dịch vụ được sử dụng trên hệ thống)*
□ Web server □ Mail server □ Database server

□ Dịch vụ khác, đó là……
• Các biện pháp an toàn thông tin mạng đã triển khai *(Đánh dấu những biện pháp đã triển khai)*
□ Antivirus
□ Firewall
□ Hệ thống phát hiện xâm nhập
□ Khác:

• Các địa chỉ IP của hệ *thống(Liệt kê địa chỉ IP sử dụng trên Internet (IP public), không liệt kê địa chỉ IP nội bộ)* ■ Các tên miền của hệ thống ■ Mục đích chính sử dụng hệ thống ■ Thông tin gửi kèm
□ Nhật ký hệ thống
□ Mẫu virus/mã độc
□ Khác:
• Các thông tin cung cấp trong thông báo sự cố này đều phải được giữ bí mật:
□ Có □ Không

IV. KIẾN NGHỊ, ĐỀ XUẤT HỖ TRỢ

Mô tả về đề xuất, kiến nghị

Đề nghị cung cấp tóm lược về các kiến nghị và đề xuất hỗ trợ ứng cứu (nếu có):

……

V. THỜI GIAN THỰC HIỆN BÁO CÁO SỰ CỐ *:

….(ngày/tháng/năm/giờ/phút)

Nơi nhận:
- Công an tỉnh;
- Lưu VT

THỦ TRƯỞNG CƠ QUAN
(Ký số)

Chú thích*: Phần (*) là những thông tin bắt buộc, các phần còn lại có thể loại bỏ nếu không có thông tin.*

(Mầu số 02)

ỦY BAN NHÂN DÂN **XÃ NGỌC LIÊN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: /BC-UBND	*Ngọc Liên, ngày ... tháng ... năm ...*

BÁO CÁO HOÀN THÀNH XỬ LÝ SỰ CỐ AN TOÀN THÔNG TIN MẠNG

I. THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN BÁO CÁO

- Tên tổ chức/cá nhân báo cáo sự cố (*)…….....
- Địa chỉ: (*)…….....
- Điện thoại (*) ……..Email (*)…….....

VĂN BẢN BÁO CÁO BAN ĐẦU SỰ CỐ:

- Số ký hiệu ……Ngày ban hành: …/.../.....

II. THÔNG TIN CHI TIẾT VỀ HỆ THỐNG BỊ SỰ CỐ

Tên đon vị vận hành hệ thống thông tin (*):	*Điền tên đơn vị vận hành hoặc được thuê vận hành hệ thống thông tin*
Co quan quản lý cấp trên:	*Điền tên cơ quan quản lý cấp trên*
Tên hệ thống bị sự cố	*Điền tên hệ thống bị sự cố*
Phân loại cấp độ của hệ thống thông tin, (nếu có)	□ Cấp độ 1 □ Cấp độ 2 □ Cấp độ 3 □ Cấp độ 4 □ Cấp độ 5

Tên/Mô tả về sự cố

Đề nghị cung cấp một bản tóm tắt ngắn gọn về sự cố, bao gồm đánh giá sơ bộ cuộc tấn công đã xảy ra chưa và bất kỳ các nguy cơ dẫn đến khả năng phá hoại hoặc gián đoạn dịch vụ. Xác định mức độ nhạy cảm của thông tin liên quan hoặc những đối tượng bị ảnh hưởng bởi sự cố. (Chỉ mô tả những cập nhật mới có thay đổi so với phần mô tả của văn bản thông báo sự cố đã gửi)

Ngày phát hiện sự cố (*) (dd/mm/yy)	…/…/.....	Thời gian phát hiện (*):	…....giờ…... phút

Kết quả xử lý sự cố

Cung cấp, tóm tắt tổng quát về những gì đã xảy ra và cách thức giải quyết, đề xuất giải pháp ứng cứu ứng sự cố nhằm xử lý nhanh sự cố, giảm nhẹ rủi ro và thiệt hại đối với sự cố tương tự trong tương lai

Các tài liệu đính kèm

Liệt kê các tài liệu liên quan (báo cáo diễn biến sự cố; phương án xử lý, log file)

Nơi nhận: - Công an tỉnh; - Lưu VT	**THỦ TRƯỞNG CƠ QUAN** **(**Ký số)

***Chú thích**: Phần (*) là những thông tin bắt buộc, các phần còn lại có thể loại bỏ nếu không có thông tin*