UBND TỈNH QUẢNG NGÃI **SỞ XÂY DỰNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 1540/QĐ-SXD	*Quảng Ngãi, ngày 06 tháng 11 năm 2026*

QUYẾT ĐỊNH

Ban hành Phương án ứng cứu sự cố an toàn thông tin, an ninh mạng đối với Hệ thống thông tin phục vụ công tác chỉ đạo, điều hành, hoạt động nội bộ của Sở Xây dựng tỉnh Quảng Ngãi

GIÁM ĐỐC SỞ XÂY DỰNG TỈNH QUẢNG NGÃI

Căn cứ Luật An ninh mạng số 116/2025/QH15 ngày 10/12/2025;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 333/2026/NĐ-CP ngày 19 tháng 8 năm 2026 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật An ninh mạng;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ ban hành 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 tháng 9 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Căn cứ Quyết định số 1744/QĐ-UBND ngày 03 tháng 12 năm 2025 của Chủ tịch Ủy ban nhân dân tỉnh Quảng Ngãi ban hành Phương án ứng cứu sự cố an toàn thông tin, an ninh mạng tỉnh Quảng Ngãi;

Căn cứ Quyết định số 1051/QĐ-UBND ngày 28 tháng 10 năm 2026 của Ủy ban nhân dân tỉnh Quảng Ngãi ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Xây dựng tỉnh Quảng Ngãi;

Căn cứ Quyết định số 2375/QĐ-CAT-ANM ngày 21/10/2026 của Công an tỉnh Quảng Ngãi về việc phê duyệt cấp độ an toàn hệ thống thông tin;

Theo đề nghị của Chánh Văn phòng Sở.

QUYẾT ĐỊNH:

Điều 1. Ban hành Phương án ứng cứu sự cố an toàn thông tin, an ninh mạng đối với Hệ thống thông tin phục vụ công tác chỉ đạo, điều hành, hoạt động nội bộ của Sở Xây dựng tỉnh Quảng Ngãi *(có Phương án kèm theo)*.

Điều 2. Các nội dung trong Phương án là căn cứ để Trưởng các phòng chuyên môn, nghiệp vụ Sở, Thủ trưởng các đơn vị thuộc Sở chủ động chỉ đạo, điều hành các hoạt động ứng phó sự cố, bảo đảm an toàn thông tin mạng; bảo

đảm hạn chế thấp nhất thiệt hại do sự cố mất an toàn an ninh thông tin gây ra đối với Hệ thống mạng nội bộ của Sở.

Điều 3. Quyết định này có hiệu lực kể từ ngày ký.

Điều 4. Chánh Văn phòng Sở; Trưởng các phòng chuyên môn, nghiệp vụ Sở; Thủ trưởng các đơn vị thuộc Sở và các đơn vị có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 4;
- Công an tỉnh (báo cáo);
- Các phòng CM NV Sở;
- Các ĐVTT Sở;
- Lưu: VT, VP

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ XÂY DỰNG
TỈNH QUẢNG NGÃI

Võ Phiến

UBND TỈNH QUẢNG NGÃI
SỞ XÂY DỰNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

PHƯƠNG ÁN
Ứng cứu sự cố an toàn thông tin, an ninh mạng đối với Hệ thống thông tin phục vụ công tác chỉ đạo, điều hành, hoạt động nội bộ của Sở Xây dựng tỉnh Quảng Ngãi

(Kèm theo Quyết định số:1540/QĐ-SXD ngày 06/11/2026 của Sở Xây dựng)

I. Mục đích, yêu cầu

1. Chủ động phòng ngừa, phát hiện, ứng phó và khắc phục kịp thời các sự cố an toàn thông tin, an ninh mạng có thể xảy ra đối với hệ thống thông tin phục vụ công tác chỉ đạo, điều hành và hoạt động nội bộ của Sở Xây dựng tỉnh Quảng Ngãi.

2. Bảo đảm tính bảo mật, tính toàn vẹn và tính sẵn sàng của hệ thống thông tin, dữ liệu và các ứng dụng phục vụ hoạt động của Sở.

3. Xác định trách nhiệm, trình tự xử lý và cơ chế phối hợp giữa các phòng, đơn vị thuộc Sở trong công tác ứng cứu sự cố; hạn chế thiệt hại, giảm thiểu thời gian gián đoạn hoạt động khi xảy ra sự cố.

4. Bảo đảm việc phối hợp với cơ quan, đơn vị chuyên trách về an toàn thông tin, an ninh mạng và các tổ chức, doanh nghiệp có liên quan trong quá trình phát hiện, xử lý, khắc phục và khôi phục hoạt động của hệ thống sau sự cố.

5. Xác định các điều kiện, nguồn lực cần thiết để tổ chức triển khai thực hiện Phương án, bảo đảm phù hợp với tình hình thực tế và điều kiện của Sở.

6. Việc ứng cứu sự cố phải kịp thời, hiệu quả, đúng thẩm quyền và tuân thủ các quy định pháp luật hiện hành về an toàn thông tin, an ninh mạng.

II. Phạm vi và đối tượng áp dụng

1. Phạm vi áp dụng: Hệ thống thông tin phục vụ công tác chỉ đạo, điều hành và hoạt động nội bộ của Sở Xây dựng tỉnh Quảng Ngãi, bao gồm hạ tầng mạng nội bộ, máy chủ, máy tính, thiết bị mạng, thiết bị đầu cuối, phần mềm, ứng dụng, dữ liệu và các tài nguyên công nghệ thông tin khác thuộc phạm vi quản lý của Sở.

2. Đối tượng áp dụng: Các phòng, đơn vị thuộc Sở; công chức, viên chức, người lao động được giao quản lý, vận hành, khai thác, sử dụng hệ thống thông tin và các tổ chức, cá nhân có liên quan trong quá trình quản lý, vận hành, bảo trì, hỗ trợ kỹ thuật đối với hệ thống thông tin của Sở.

3. Các sự cố an toàn thông tin, an ninh mạng phát sinh trong quá trình quản lý, vận hành và sử dụng hệ thống thông tin thuộc phạm vi áp dụng của Phương án, bao gồm sự cố liên quan đến phần cứng, phần mềm, mạng máy tính, dữ liệu, tài khoản người dùng, mã độc, truy cập trái phép và các nguy cơ khác ảnh hưởng đến hoạt động bình thường của hệ thống.

III. Cơ cấu lực lượng ứng cứu sự cố tại Sở Xây dựng

1. Cơ cấu lực lượng ứng cứu sự cố.

1.1. Đội Ứng cứu sự cố an toàn thông tin mạng nội bộ Sở Xây dựng tỉnh Quảng Ngãi được thành lập tại Quyết định số 631/QĐ-SXD ngày 18/4/2026 của Sở Xây dựng, là lực lượng nòng cốt thực hiện công tác ứng cứu sự cố an toàn thông tin, an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý của Sở.

1.2. Công chức, viên chức, người lao động thuộc các phòng, đơn vị của Sở có trách nhiệm phối hợp phát hiện, thông báo sự cố và thực hiện các nhiệm vụ ứng cứu theo phân công; kịp thời báo cáo khi phát hiện dấu hiệu mất an toàn thông tin, an ninh mạng.

1.3. Các cơ quan, đơn vị chuyên trách về an toàn thông tin, an ninh mạng và các tổ chức, doanh nghiệp có liên quan phối hợp, hỗ trợ Sở Xây dựng trong quá trình xử lý, khắc phục và khôi phục hệ thống khi xảy ra sự cố theo chức năng, nhiệm vụ và thẩm quyền.

2. Hoạt động của lực lượng ứng cứu sự cố

2.1. Đội Ứng cứu sự cố nội bộ Sở Xây dựng

- Thực hiện nhiệm vụ phát hiện, xử lý ban đầu, phối hợp ứng cứu và khắc phục sự cố an toàn thông tin, an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý của Sở Xây dựng.

- Hoạt động dưới sự chỉ đạo của lãnh đạo Sở; phối hợp với các phòng, đơn vị thuộc Sở và cơ quan, đơn vị chuyên trách về an toàn thông tin, an ninh mạng trong quá trình tiếp nhận, xử lý, khắc phục và báo cáo sự cố.

- Chủ động rà soát các nguy cơ mất an toàn thông tin, lỗ hổng bảo mật trên hệ thống thông tin thuộc phạm vi quản lý; kịp thời tham mưu, đề xuất biện pháp khắc phục theo hướng dẫn, cảnh báo của cơ quan chức năng.

- Có trách nhiệm:

(1) Tham mưu xây dựng, rà soát, cập nhật Phương án ứng cứu sự cố an toàn thông tin, an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý của Sở.

(2) Tiếp nhận thông tin về sự cố từ hệ thống, người sử dụng hoặc các cơ quan, đơn vị có liên quan.

(3) Đánh giá sơ bộ tình hình, mức độ ảnh hưởng; tổ chức xử lý ban đầu, triển khai các biện pháp cần thiết để hạn chế thiệt hại và ngăn ngừa sự cố lan rộng.

(4) Phối hợp với các phòng, đơn vị thuộc Sở và cơ quan, đơn vị chuyên trách về an toàn thông tin, an ninh mạng trong quá trình xử lý, khắc phục và khôi phục hoạt động của hệ thống sau sự cố.

(5) Tổng hợp tình hình, diễn biến, kết quả xử lý sự cố; tham mưu lãnh đạo Sở thực hiện báo cáo theo quy định.

2.2. Trách nhiệm của các phòng, đơn vị và cá nhân thuộc Sở

- Chủ động phát hiện, kịp thời thông báo cho Đội Ứng cứu sự cố nội bộ khi phát hiện dấu hiệu hoặc xảy ra sự cố an toàn thông tin, an ninh mạng trong quá trình quản lý, khai thác, sử dụng hệ thống thông tin.

- Phối hợp với Đội Ứng cứu sự cố nội bộ trong quá trình xác minh, xử lý, khắc phục sự cố; cung cấp đầy đủ thông tin có liên quan theo yêu cầu.

- Chấp hành hướng dẫn, yêu cầu xử lý sự cố của lãnh đạo Sở và Đội Ứng cứu sự cố nội bộ; không tự ý thực hiện các thao tác có thể làm mất dữ liệu, ảnh hưởng đến việc xác định nguyên nhân và xử lý sự cố.

- Thực hiện các biện pháp bảo đảm an toàn thông tin, an ninh mạng theo quy định và hướng dẫn của Sở; chịu trách nhiệm về việc quản lý, sử dụng tài khoản, thiết bị và dữ liệu được giao.

IV. QUY TRÌNH ỨNG CỨU SỰ CỐ

1. Phát hiện, tiếp nhận và báo cáo

1.1. Khi phát hiện dấu hiệu bất thường hoặc sự cố an toàn thông tin, an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý của Sở Xây dựng, công chức, viên chức, người lao động phải kịp thời thông báo cho Đội Ứng cứu sự cố nội bộ hoặc cá nhân được giao quản lý, vận hành hệ thống để tiếp nhận, kiểm tra và xử lý ban đầu.

1.2. Đội Ứng cứu sự cố nội bộ có trách nhiệm tiếp nhận thông tin, ghi nhận thời điểm phát hiện, hiện trạng, dấu hiệu và phạm vi ảnh hưởng của sự cố; tổ chức kiểm tra, đánh giá sơ bộ, triển khai biện pháp xử lý ban đầu và báo cáo lãnh đạo Sở theo quy định. Trường hợp tiếp nhận thông tin từ công chức, viên chức, người lao động hoặc đơn vị liên quan, phải xác nhận việc tiếp nhận thông tin để phối hợp xử lý.

1.3. Đối với sự cố nghiêm trọng hoặc có nguy cơ ảnh hưởng đến an toàn thông tin, an ninh mạng, Đội Ứng cứu sự cố nội bộ kịp thời tham mưu lãnh đạo Sở báo cáo cơ quan chuyên trách về an toàn thông tin, an ninh mạng và cơ quan điều phối ứng cứu sự cố theo quy định; bảo đảm thời hạn báo cáo không quá 24 giờ kể từ thời điểm phát hiện hoặc tiếp nhận thông tin về sự cố đối với trường hợp thuộc diện phải báo cáo.

Nội dung báo cáo gồm:

+ Tên, địa chỉ đơn vị, cá nhân vận hành hệ thống thông tin;

+ Cơ quan chủ quản hệ thống thông tin;

+ Hệ thống thông tin bị sự cố;

+ Thời điểm phát hiện sự cố;

+ Đầu mối liên lạc về sự cố của đơn vị, cá nhân vận hành hệ thống bị sự cố;

+ Đơn vị cung cấp dịch vụ hạ tầng công nghệ thông tin, viễn thông;

+ Các tổ chức, doanh nghiệp đang hỗ trợ ứng cứu, xử lý;

+ Mô tả về sự cố theo các thông tin (loại sự cố, hiện tượng, đánh giá sơ bộ mức độ nguy hại, mức độ lây lan, tác động của sự cố đến hoạt động bình thường của tổ chức);

+ Các biện pháp đã triển khai hoặc dự kiến triển khai để xử lý khắc phục sự cố;

+ Kết quả xử lý sự cố tính đến thời điểm báo cáo;

+ Kiến nghị đề xuất hướng ứng cứu xử lý sự cố (nếu có).

1.4. Đội Ứng cứu sự cố nội bộ có trách nhiệm theo dõi, cập nhật diễn biến và kết quả xử lý sự cố; phối hợp với các phòng, đơn vị thuộc Sở và cơ quan, đơn vị liên quan trong quá trình ứng cứu. Trường hợp sự cố nghiêm trọng hoặc vượt quá khả năng xử lý, kịp thời báo cáo lãnh đạo Sở để chỉ đạo và đề nghị hỗ trợ theo quy định.

1.5. Trong quá trình xử lý sự cố, các phòng, đơn vị và cá nhân liên quan có trách nhiệm phối hợp, cung cấp thông tin và thực hiện các yêu cầu cần thiết để phục vụ công tác ứng cứu; không tự ý cung cấp thông tin về sự cố cho tổ chức, cá nhân không có trách nhiệm khi chưa được cấp có thẩm quyền cho phép.

- Đơn vị chủ trì: Đội Ứng cứu sự cố nội bộ Sở Xây dựng.

- Đơn vị phối hợp: Các phòng, đơn vị thuộc Sở; cơ quan, đơn vị chuyên trách về an toàn thông tin, an ninh mạng và tổ chức, doanh nghiệp cung cấp dịch vụ công nghệ thông tin có liên quan (nếu có).

2. Ứng phó sự cố ban đầu

Đội Ứng cứu sự cố nội bộ Sở Xây dựng chủ trì, phối hợp với cá nhân, đơn vị được giao quản lý, vận hành hệ thống thông tin và các tổ chức, doanh nghiệp cung cấp dịch vụ công nghệ thông tin có liên quan (nếu có) tiến hành kiểm tra, phân tích, xác minh, đánh giá sự cố; xác định nguyên nhân, phạm vi ảnh hưởng và triển khai các biện pháp xử lý ban đầu phù hợp với tính chất, mức độ sự cố.

Việc ứng phó sự cố được thực hiện theo Phương án đã được Sở phê duyệt và các quy định hiện hành, tập trung vào các nội dung sau:

- Xác định nguyên nhân, nguồn gốc và mức độ ảnh hưởng của sự cố, tập trung vào các tình huống thường gặp như:

+ Hệ thống thông tin bị tấn công, truy cập trái phép, chiếm quyền điều khiển, cài đặt mã độc, thay đổi giao diện hoặc phá hoại dữ liệu, phần mềm;

+ Tài khoản người dùng, tài khoản quản trị bị lộ, mất hoặc bị chiếm quyền sử dụng;

+ Thông tin, dữ liệu thuộc phạm vi quản lý của Sở, trong đó có thông tin cá nhân, tài liệu nội bộ, tài liệu bí mật nhà nước bị lộ, mất hoặc bị truy cập trái phép;

+ Hệ thống thông tin, máy chủ, thiết bị mạng, máy tính và các thiết bị công nghệ thông tin hoạt động bất thường, bị gián đoạn hoặc không thể truy cập;

+ Sự cố do lỗi phần cứng, phần mềm, hạ tầng kỹ thuật, nguồn điện, đường truyền Internet hoặc lỗi trong quá trình quản lý, vận hành, sử dụng hệ thống;

+ Sự cố do thiên tai, hỏa hoạn và các nguyên nhân khác ảnh hưởng đến hoạt động bình thường của hệ thống thông tin.

- Thực hiện các biện pháp ngăn chặn, cô lập sự cố: Ngắt kết nối thiết bị, máy tính hoặc hệ thống bị nhiễm mã độc, bị tấn công khi cần thiết; khóa tài khoản có dấu hiệu bị xâm nhập; chặn các địa chỉ IP, kết nối hoặc nguồn truy cập nghi ngờ độc hại để hạn chế sự cố lây lan, phát sinh thiệt hại.

- Bảo vệ dữ liệu và duy trì hoạt động của hệ thống: Thực hiện sao lưu, bảo toàn dữ liệu và thông tin liên quan đến sự cố; trường hợp cần thiết, triển khai khôi phục hệ thống từ bản sao lưu an toàn hoặc chuyển sang thiết bị, hạ tầng dự phòng (nếu có).

- Đề nghị hỗ trợ xử lý sự cố: Trường hợp sự cố nghiêm trọng, có dấu hiệu tấn công có chủ đích hoặc vượt quá khả năng xử lý của Đội Ứng cứu sự cố nội bộ, tham mưu lãnh đạo Sở báo cáo, đề nghị cơ quan chuyên trách về an toàn thông tin, an ninh mạng và các tổ chức, doanh nghiệp có chuyên môn hỗ trợ kiểm tra, điều tra, xử lý và khắc phục sự cố.

- Tăng cường giám sát hệ thống: Theo dõi tình trạng hoạt động của hệ thống trong suốt quá trình xử lý; kiểm tra, đánh giá hiệu quả các biện pháp ngăn chặn, kịp thời phát hiện các dấu hiệu tấn công hoặc nguy cơ mất an toàn thông tin phát sinh.

- Đơn vị chủ trì: Đội Ứng cứu sự cố nội bộ Sở Xây dựng.

- Đơn vị phối hợp: Các phòng, đơn vị thuộc Sở và tổ chức, doanh nghiệp cung cấp dịch vụ công nghệ thông tin có liên quan (nếu có).

3. Phân tích tính chất và đánh giá mức độ khi xảy ra sự cố

Sau khi thực hiện các biện pháp ứng phó ban đầu, Đội Ứng cứu sự cố nội bộ Sở Xây dựng phối hợp với các cá nhân, đơn vị có liên quan tiến hành phân tích, xác minh nguyên nhân, đánh giá phạm vi ảnh hưởng và phân loại mức độ nghiêm trọng của sự cố để xác định biện pháp xử lý phù hợp, cụ thể như sau:

Mức 1: Sự cố ít nghiêm trọng. Phạm vi ảnh hưởng cục bộ, không ảnh hưởng đáng kể đến hoạt động của hệ thống thông tin; chưa có dấu hiệu lộ, mất dữ liệu hoặc truy cập trái phép. Đội Ứng cứu sự cố nội bộ chủ động kiểm tra, xử lý và khắc phục theo quy trình, phương án đã được phê duyệt; ghi nhận diễn biến, biện pháp và kết quả xử lý sự cố.

Mức 2: Sự cố nghiêm trọng trung bình. Sự cố gây gián đoạn một phần hoạt động của hệ thống thông tin, có dấu hiệu truy cập trái phép, nguy cơ lộ, mất dữ liệu hoặc phạm vi ảnh hưởng chưa được xác định đầy đủ. Đội Ứng cứu sự cố nội bộ tổ chức khoanh vùng, triển khai biện pháp ngăn chặn, khắc phục; đồng thời báo cáo lãnh đạo Sở và đề nghị cơ quan, đơn vị chuyên trách về an toàn thông tin, an ninh mạng hỗ trợ khi cần thiết.

Mức 3: Sự cố nghiêm trọng. Sự cố gây gián đoạn hoạt động của hệ thống thông tin, có dấu hiệu bị tấn công có chủ đích, chiếm quyền quản trị, phá hoại hệ thống, lộ, mất dữ liệu quan trọng hoặc tài liệu bí mật nhà nước; phạm vi ảnh hưởng lớn hoặc vượt quá khả năng xử lý của Đội Ứng cứu sự cố nội bộ. Đội Ứng cứu sự cố nội bộ phải kịp thời báo cáo lãnh đạo Sở để chỉ đạo, đồng thời đề nghị cơ quan chuyên trách về an toàn thông tin, an ninh mạng và các tổ chức, doanh nghiệp có chuyên môn phối hợp điều tra, xử lý, khắc phục và khôi phục hoạt động của hệ thống.

Việc đánh giá, phân loại mức độ sự cố phải căn cứ vào tính chất, mức độ ảnh hưởng thực tế, phạm vi tác động và khả năng xử lý của Đội Ứng cứu sự cố nội bộ; trường hợp cần thiết, thực hiện đánh giá lại trong quá trình ứng cứu để kịp thời điều chỉnh biện pháp xử lý.

4. Thu thập dữ liệu, điều tra nguyên nhân sự cố

- Đội Ứng cứu sự cố nội bộ Sở Xây dựng chủ trì, phối hợp với các phòng, đơn vị thuộc Sở và tổ chức, doanh nghiệp có liên quan (nếu có) thực hiện thu thập thông tin, dữ liệu, nhật ký hệ thống và các tài liệu liên quan đến sự cố; bảo toàn hiện trạng hệ thống, dữ liệu phục vụ việc xác minh, phân tích và điều tra nguyên nhân sự cố.

- Các phòng, đơn vị và cá nhân có liên quan có trách nhiệm phối hợp, cung cấp đầy đủ thông tin, dữ liệu theo yêu cầu của Đội Ứng cứu sự cố nội bộ; không tự ý xóa, sửa đổi hoặc làm thay đổi dữ liệu, nhật ký và các thông tin có liên quan đến sự cố.

- Trên cơ sở thông tin, dữ liệu thu thập được, Đội Ứng cứu sự cố nội bộ tiến hành phân tích, xác định nguyên nhân, phương thức và nguồn gốc phát sinh sự cố; đánh giá các lỗ hổng, điểm yếu trong hệ thống để đề xuất biện pháp khắc phục triệt để, phòng ngừa sự cố tái diễn.

- Trường hợp sự cố phức tạp, vượt quá khả năng chuyên môn, Đội Ứng cứu sự cố nội bộ tham mưu lãnh đạo Sở đề nghị cơ quan chuyên trách về an toàn thông tin, an ninh mạng hoặc tổ chức, doanh nghiệp có chuyên môn hỗ trợ thu thập, phân tích dữ liệu và xác định nguyên nhân sự cố.

5. Xử lý sự cố, gỡ bỏ và khắc phục

Mục tiêu của giai đoạn này là loại bỏ nguyên nhân gây ra sự cố, khắc phục các lỗ hổng, điểm yếu và khôi phục hoạt động bình thường, bảo đảm an toàn cho hệ thống thông tin thuộc phạm vi quản lý của Sở Xây dựng.

- Đội Ứng cứu sự cố nội bộ Sở Xây dựng chủ trì, phối hợp với các phòng, đơn vị và cá nhân có liên quan triển khai các biện pháp xử lý, khắc phục sự cố phù hợp, bao gồm: rà quét, phát hiện và gỡ bỏ mã độc, phần mềm độc hại; cô lập thiết bị bị ảnh hưởng; khắc phục lỗ hổng bảo mật; thay đổi mật khẩu, thu hồi tài khoản bị xâm nhập; rà soát, điều chỉnh quyền truy cập; cấu hình lại các thiết bị, hệ thống bảo mật và cập nhật phần mềm cần thiết.

- Đối với hệ thống, dữ liệu bị ảnh hưởng, thực hiện khôi phục từ các bản

sao lưu an toàn, bảo đảm tính toàn vẹn của dữ liệu trước khi đưa vào sử dụng. Trước khi khôi phục hoạt động chính thức, phải kiểm tra, đánh giá tình trạng an toàn của hệ thống, bảo đảm các nguyên nhân gây ra sự cố đã được khắc phục.

- Trường hợp sự cố vượt quá khả năng xử lý, Đội Ứng cứu sự cố nội bộ tham mưu lãnh đạo Sở đề nghị cơ quan chuyên trách về an toàn thông tin, an ninh mạng hoặc tổ chức, doanh nghiệp có chuyên môn hỗ trợ triển khai các biện pháp kỹ thuật để xử lý, khắc phục và khôi phục hệ thống.

- Sau khi khắc phục sự cố, Đội Ứng cứu sự cố nội bộ phối hợp với cá nhân, đơn vị quản lý, vận hành hệ thống kiểm tra hoạt động, tăng cường giám sát để kịp thời phát hiện nguy cơ tái diễn; đồng thời đề xuất các giải pháp nâng cao năng lực bảo đảm an toàn thông tin, an ninh mạng đối với hệ thống thông tin của Sở.

6. Kiểm tra, đánh giá hệ thống thông tin sau khắc phục sự cố

Đội Ứng cứu sự cố nội bộ Sở Xây dựng chủ trì, phối hợp với cá nhân, đơn vị được giao quản lý, vận hành hệ thống và các tổ chức, doanh nghiệp có liên quan (nếu có) thực hiện kiểm tra, đánh giá tình trạng hoạt động và mức độ an toàn của hệ thống thông tin sau khi khắc phục sự cố; kiểm tra tính toàn vẹn của dữ liệu, hiệu quả của các biện pháp bảo mật và phòng, chống mã độc trước khi đưa hệ thống trở lại hoạt động bình thường.

Trường hợp hệ thống chưa hoạt động ổn định hoặc vẫn còn dấu hiệu mất an toàn thông tin, Đội Ứng cứu sự cố nội bộ tiếp tục phối hợp xác minh nguyên nhân, đánh giá phạm vi ảnh hưởng và triển khai các biện pháp xử lý, khắc phục cần thiết cho đến khi hệ thống hoạt động ổn định, bảo đảm an toàn.

7. Báo cáo tổng kết, đánh giá và rút kinh nghiệm

Sau khi sự cố được xử lý và hệ thống thông tin hoạt động ổn định trở lại, Đội Ứng cứu sự cố nội bộ Sở Xây dựng có trách nhiệm tổng hợp, tham mưu lãnh đạo Sở báo cáo kết quả xử lý sự cố theo quy định hoặc khi có yêu cầu của cơ quan có thẩm quyền.

Nội dung báo cáo cần nêu rõ: thời gian, diễn biến sự cố; nguyên nhân, phạm vi và mức độ ảnh hưởng; các biện pháp đã triển khai; kết quả xử lý, khắc phục; thiệt hại (nếu có) và đề xuất, khuyến nghị phòng ngừa.

Đội Ứng cứu sự cố nội bộ phối hợp với các phòng, đơn vị có liên quan tổ chức đánh giá, rút kinh nghiệm trong công tác quản lý, vận hành và xử lý sự cố; đề xuất các giải pháp khắc phục hạn chế, phòng ngừa sự cố tương tự, rà soát, cập nhật Phương án ứng cứu sự cố và các biện pháp bảo đảm an toàn thông tin, an ninh mạng của Sở.

Các thông tin, tài liệu và hồ sơ liên quan đến sự cố phải được tổng hợp, lưu trữ đầy đủ theo quy định để phục vụ công tác quản lý, theo dõi, kiểm tra khi cần thiết.