UBND TỈNH QUẢNG NGÃI
SỞ XÂY DỰNG

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

Số: 8989/KH-SXD

Quảng Ngãi, ngày 05 tháng 11 năm 2026

KẾ HOẠCH
Triển khai thực hiện công tác bảo đảm an ninh mạng, an ninh dữ liệu Quý IV năm 2026 tại Sở Xây dựng

Theo Kế hoạch số 8881/KH-TANM ngày 03/11/2026 của Tổ Công tác về An ninh mạng Ban Chỉ đạo 57 tỉnh Quảng Ngãi về hoạt động của Tổ Công tác về An ninh mạng Ban Chỉ đạo 57 tỉnh Quý IV/2026, Sở Xây dựng ban hành Kế hoạch triển khai thực hiện như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

-Tổ chức triển khai thực hiện nghiêm túc, hiệu quả các nhiệm vụ về bảo đảm an ninh mạng, an ninh dữ liệu theo chỉ đạo của Ban Chỉ đạo 57 tỉnh; nâng cao trách nhiệm của công chức, viên chức, người lao động trong công tác bảo đảm an toàn thông tin mạng tại cơ quan, đơn vị.

- Chủ động rà soát, đánh giá và triển khai các biện pháp bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin, cơ sở dữ liệu, hạ tầng công nghệ thông tin thuộc phạm vi quản lý, sử dụng của Sở; phòng ngừa nguy cơ mất an toàn thông tin, lộ lọt dữ liệu và bí mật nhà nước.

- Nâng cao nhận thức, kỹ năng sử dụng các hệ thống thông tin, nền tảng số an toàn; bảo đảm hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của Sở được thực hiện an toàn, liên tục và đúng quy định.

2. Yêu cầu

- Việc triển khai phải bám sát chức năng, nhiệm vụ, quyền hạn của Sở Xây dựng; tập trung vào các hệ thống thông tin, cơ sở dữ liệu, thiết bị và hoạt động ứng dụng công nghệ thông tin thuộc phạm vi quản lý, sử dụng của Sở.

- Xác định rõ trách nhiệm của Văn phòng Sở, các phòng chuyên môn, nghiệp vụ và các đơn vị trực thuộc trong quản lý, khai thác, sử dụng, bảo vệ hệ thống thông tin và dữ liệu được giao.

- Thực hiện phương châm chủ động phòng ngừa, phát hiện và xử lý kịp thời nguy cơ mất an toàn thông tin; kết hợp giữa biện pháp quản lý, kỹ thuật và nâng cao ý thức trách nhiệm của người sử dụng.

- Bảo đảm nguyên tắc rõ người, rõ việc, rõ trách nhiệm, rõ tiến độ và rõ kết quả thực hiện; kịp thời báo cáo, phối hợp xử lý những vấn đề vượt thẩm quyền.

II. NỘI DUNG NHIỆM VỤ

1. Tăng cường công tác lãnh đạo, chỉ đạo và trách nhiệm trong bảo đảm an ninh mạng

- Quán triệt, triển khai các nội dung của Kế hoạch hoạt động của Tổ Công tác về An ninh mạng Ban Chỉ đạo 57 tỉnh Quý IV/2026 đến công chức, viên chức, người lao động thuộc Sở; nâng cao trách nhiệm của người đứng đầu các phòng, đơn vị trong công tác bảo đảm an ninh mạng, an toàn thông tin và bảo vệ dữ liệu.

- Rà soát, xác định rõ trách nhiệm của các phòng, đơn vị và cá nhân được giao quản lý, vận hành, khai thác hệ thống thông tin, cơ sở dữ liệu; phân công đầu mối phụ trách công tác an toàn thông tin tại cơ quan Sở và các đơn vị trực thuộc.

- Tăng cường kiểm tra việc chấp hành các quy định về quản lý, sử dụng thiết bị công nghệ thông tin, tài khoản truy cập, phần mềm và các hệ thống thông tin trong quá trình thực hiện nhiệm vụ.

2. Rà soát, bảo đảm an toàn hệ thống thông tin, hạ tầng công nghệ thông tin

- Rà soát tổng thể hiện trạng hạ tầng công nghệ thông tin tại cơ quan Sở, gồm hệ thống mạng LAN, mạng truyền số liệu chuyên dùng, đường truyền Internet, máy chủ, máy tính, thiết bị mạng, thiết bị bảo mật và các thiết bị công nghệ thông tin khác; kịp thời phát hiện, khắc phục những tồn tại, nguy cơ gây mất an toàn thông tin.

- Kiểm tra, rà soát việc quản lý, vận hành hệ thống tường lửa, phần mềm phòng, chống mã độc, phần mềm bảo vệ thiết bị đầu cuối; bảo đảm các thiết bị được cập nhật bản vá bảo mật, cơ sở dữ liệu nhận diện mã độc và các phiên bản phần mềm theo quy định.

- Rà soát tài khoản người dùng, tài khoản quản trị và quyền truy cập các hệ thống thông tin; thực hiện cấp, điều chỉnh, thu hồi tài khoản và phân quyền phù hợp với chức năng, nhiệm vụ của từng cá nhân; không sử dụng chung tài khoản, không chia sẻ thông tin xác thực truy cập.

- Kiểm tra việc thực hiện sao lưu dữ liệu, bảo đảm khả năng phục hồi dữ liệu khi xảy ra sự cố; quản lý chặt chẽ các thiết bị lưu trữ, thiết bị ngoại vi và việc kết nối các thiết bị vào hệ thống mạng nội bộ.

- Tiếp tục thực hiện các quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ đối với hệ thống thông tin thuộc phạm vi quản lý của Sở; rà soát, duy trì các biện pháp bảo vệ phù hợp với cấp độ an toàn thông tin đã được phê duyệt.

- Đối với các hệ thống thông tin, nền tảng số và cơ sở dữ liệu do cơ quan cấp trên hoặc đơn vị khác quản lý, vận hành, Sở thực hiện đúng trách nhiệm trong phạm vi được phân quyền sử dụng; quản lý chặt chẽ tài khoản, thiết bị và dữ liệu truy cập, đồng thời phối hợp với cơ quan quản lý hệ thống khi phát sinh

vấn đề về an toàn thông tin.

3. Bảo đảm an ninh dữ liệu, bảo vệ dữ liệu cá nhân và bí mật nhà nước

- Rà soát việc quản lý, khai thác, sử dụng, lưu trữ và chia sẻ dữ liệu trong quá trình thực hiện nhiệm vụ chuyên môn; chú trọng các cơ sở dữ liệu thuộc lĩnh vực xây dựng, giao thông vận tải, nhà ở và thị trường bất động sản, quy hoạch xây dựng, hạ tầng kỹ thuật đô thị và các dữ liệu khác thuộc phạm vi quản lý của Sở.

- Kiểm soát việc thu thập, xử lý, lưu trữ, cung cấp và chia sẻ dữ liệu cá nhân trong các hoạt động thuộc phạm vi quản lý của Sở; bảo đảm đúng mục đích, đúng thẩm quyền, đúng đối tượng và tuân thủ quy định về bảo vệ dữ liệu cá nhân.

- Thực hiện nghiêm các quy định về bảo vệ bí mật nhà nước trong quá trình soạn thảo, lưu trữ, trao đổi và khai thác thông tin, tài liệu; không sử dụng hệ thống, thiết bị, phần mềm hoặc nền tảng không đáp ứng yêu cầu bảo mật để xử lý, lưu trữ, trao đổi tài liệu bí mật nhà nước.

- Tăng cường quản lý việc sử dụng thư điện tử công vụ, phần mềm quản lý văn bản và điều hành, các nền tảng trao đổi thông tin và thiết bị lưu trữ; không tự ý cung cấp, phát tán dữ liệu, tài liệu nội bộ của cơ quan khi chưa được phép.

- Rà soát, chấn chỉnh việc quản lý, khai thác dữ liệu và quyền truy cập của các cá nhân được giao nhiệm vụ; kịp thời thu hồi quyền truy cập khi thay đổi vị trí công tác hoặc không còn nhiệm vụ liên quan.

4. Bảo đảm an ninh mạng trong ứng dụng công nghệ thông tin và chuyển đổi số

- Trong quá trình đề xuất, xây dựng, nâng cấp, đầu tư, thuê dịch vụ và đưa vào khai thác các hệ thống thông tin, cơ sở dữ liệu thuộc phạm vi quản lý của Sở, phải quan tâm yêu cầu bảo đảm an ninh mạng, an toàn thông tin ngay từ khâu đề xuất, thiết kế, triển khai và vận hành; thực hiện các quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ trước khi đưa vào khai thác, sử dụng.

- Rà soát các nhiệm vụ, dự án ứng dụng công nghệ thông tin, chuyển đổi số do Sở chủ trì tham mưu hoặc tổ chức thực hiện; bảo đảm nội dung, giải pháp và kinh phí cho công tác an toàn thông tin được xem xét, bố trí theo quy định và hướng dẫn của cơ quan có thẩm quyền.

- Tăng cường kiểm soát việc sử dụng các phần mềm, ứng dụng, nền tảng số và công cụ trí tuệ nhân tạo (AI) trong hoạt động chuyên môn; không đưa thông tin, dữ liệu cá nhân, tài liệu nội bộ hoặc bí mật nhà nước lên các nền tảng, ứng dụng khi chưa được phép hoặc chưa bảo đảm yêu cầu an toàn, bảo mật.

- Đối với các hệ thống thông tin, cơ sở dữ liệu do Sở quản lý, vận hành, chủ động rà soát các yêu cầu bảo mật trong quá trình khai thác, sử dụng; kịp thời đề xuất biện pháp khắc phục hoặc báo cáo cấp có thẩm quyền đối với các nội dung vượt khả năng xử lý của Sở.

5. Nâng cao nhận thức, kỹ năng bảo đảm an toàn thông tin mạng

- Tổ chức phổ biến, tuyên truyền các quy định, hướng dẫn về an ninh mạng, an toàn thông tin, bảo vệ dữ liệu cá nhân và bảo vệ bí mật nhà nước đến công chức, viên chức, người lao động thuộc Sở.

- Quán triệt việc chấp hành các quy định về sử dụng máy tính, thiết bị công nghệ thông tin; không truy cập đường dẫn, tập tin không rõ nguồn gốc; không cài đặt phần mềm không được phép; không cung cấp mật khẩu, mã xác thực và thông tin tài khoản cho người khác.

- Yêu cầu người sử dụng khóa màn hình máy tính khi rời khỏi vị trí làm việc và tắt máy tính khi kết thúc giờ làm việc, trừ các thiết bị được giao vận hành liên tục, phục vụ nhiệm vụ kỹ thuật hoặc sao lưu dữ liệu theo yêu cầu.

- Khuyến khích công chức, viên chức, người lao động chủ động cập nhật kiến thức, kỹ năng nhận diện, phòng ngừa các hình thức tấn công mạng, lừa đảo trực tuyến và các nguy cơ mất an toàn thông tin trong quá trình sử dụng Internet, thư điện tử và các nền tảng số.

6. Chủ động phòng ngừa, phát hiện và phối hợp xử lý sự cố an ninh mạng

- Thường xuyên theo dõi tình trạng hoạt động của hệ thống thông tin, thiết bị công nghệ thông tin; kịp thời phát hiện các dấu hiệu bất thường, nguy cơ bị tấn công mạng, lây nhiễm mã độc, truy cập trái phép hoặc mất an toàn dữ liệu.

- Đối với hệ thống thông tin tại cơ quan Sở, Văn phòng Sở là đầu mối tiếp nhận thông tin về sự cố an toàn thông tin; phối hợp với công chức, cá nhân được Giám đốc Sở phân công phụ trách kỹ thuật, an ninh mạng để kiểm tra, xử lý theo chức năng, nhiệm vụ được giao.

- Đối với hệ thống thông tin, cơ sở dữ liệu do các đơn vị trực thuộc quản lý, vận hành, thủ trưởng đơn vị chịu trách nhiệm tổ chức kiểm tra, xử lý ban đầu và báo cáo kịp thời về Sở khi phát sinh sự cố hoặc nguy cơ mất an toàn thông tin.

- Khi phát hiện sự cố có nguy cơ ảnh hưởng đến an ninh mạng, an toàn dữ liệu hoặc hoạt động của hệ thống thông tin, các phòng, đơn vị và cá nhân liên quan phải kịp thời thông báo đầu mối phụ trách; phối hợp thực hiện biện pháp ngăn chặn, hạn chế thiệt hại, bảo vệ dữ liệu và khôi phục hoạt động hệ thống theo hướng dẫn chuyên môn.

- Trường hợp sự cố vượt khả năng xử lý hoặc có dấu hiệu liên quan đến tấn công mạng, lộ lọt dữ liệu, bí mật nhà nước, Sở kịp thời báo cáo và phối hợp với Công an tỉnh, Sở Khoa học và Công nghệ và cơ quan có thẩm quyền để được hướng dẫn, hỗ trợ xử lý theo quy định.

III. TIẾN ĐỘ THỰC HIỆN

1. Từ ngày ban hành Kế hoạch đến ngày 15/11/2026

- Các phòng, đơn vị tổ chức phổ biến, quán triệt Kế hoạch đến công chức, viên chức, người lao động.

- Rà soát, xác định đầu mối và trách nhiệm của các phòng, đơn vị, cá nhân trong công tác bảo đảm an ninh mạng, an toàn thông tin.

- Tổ chức rà soát ban đầu hiện trạng hạ tầng công nghệ thông tin, hệ thống thông tin, cơ sở dữ liệu thuộc phạm vi quản lý, sử dụng.

2. Từ ngày 16/11/2026 đến ngày 15/12/2026

- Tập trung triển khai các biện pháp bảo đảm an toàn hệ thống thông tin, hạ tầng công nghệ thông tin; rà soát tài khoản, phân quyền, sao lưu dữ liệu và các biện pháp bảo vệ thiết bị đầu cuối.

- Rà soát việc quản lý, khai thác, sử dụng dữ liệu cá nhân, dữ liệu chuyên ngành và tài liệu có nội dung bí mật nhà nước.

- Tổ chức tuyên truyền, phổ biến các quy định và kỹ năng bảo đảm an toàn thông tin cho công chức, viên chức, người lao động.

- Kịp thời khắc phục các tồn tại thuộc thẩm quyền; báo cáo, đề xuất xử lý đối với các nội dung vượt thẩm quyền.

3. Từ ngày 16/12/2026 đến ngày 31/12/2026

- Tiếp tục duy trì các biện pháp bảo đảm an ninh mạng, an toàn thông tin; kiểm tra việc thực hiện các nhiệm vụ đã đề ra.

- Tổng hợp, đánh giá kết quả thực hiện Kế hoạch; báo cáo cấp có thẩm quyền khi có yêu cầu.

IV. TỔ CHỨC THỰC HIỆN

1. Văn phòng Sở

- Là đầu mối tham mưu Lãnh đạo Sở tổ chức triển khai, theo dõi, đôn đốc việc thực hiện Kế hoạch này; hướng dẫn các phòng, đơn vị thực hiện các nội dung liên quan đến bảo đảm an ninh mạng, an toàn thông tin trong phạm vi chức năng, nhiệm vụ được giao.

- Chủ trì rà soát hiện trạng hạ tầng công nghệ thông tin, mạng nội bộ, máy chủ, thiết bị bảo mật, thiết bị đầu cuối và các hệ thống thông tin tại cơ quan Sở; phối hợp với cá nhân được phân công phụ trách kỹ thuật, an ninh mạng đề xuất biện pháp bảo đảm an toàn thông tin.

- Tham mưu Giám đốc Sở phân công bằng văn bản công chức, cá nhân phụ trách kỹ thuật, an ninh mạng tại cơ quan Sở; làm đầu mối tiếp nhận, phối hợp xử lý thông tin về sự cố an toàn thông tin.

- Theo dõi, tổng hợp kết quả thực hiện của các phòng, đơn vị; tham mưu Sở báo cáo cơ quan có thẩm quyền theo quy định.

2. Các phòng chuyên môn, nghiệp vụ thuộc Sở

- Căn cứ chức năng, nhiệm vụ được giao, tổ chức thực hiện các nội dung của Kế hoạch; chịu trách nhiệm về việc quản lý, khai thác, sử dụng và bảo vệ thông tin, dữ liệu thuộc lĩnh vực phụ trách.

- Rà soát việc quản lý, sử dụng tài khoản, quyền truy cập, dữ liệu chuyên ngành và các hệ thống thông tin phục vụ công tác chuyên môn; kịp thời thông báo cho Văn phòng Sở khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin.

- Quán triệt công chức thuộc phòng chấp hành nghiêm các quy định về an ninh mạng, an toàn thông tin, bảo vệ dữ liệu cá nhân và bí mật nhà nước.

3. Các đơn vị trực thuộc Sở

- Căn cứ chức năng, nhiệm vụ và phạm vi quản lý, vận hành hệ thống thông tin, cơ sở dữ liệu của đơn vị, chủ động triển khai các biện pháp bảo đảm an ninh mạng, an toàn thông tin theo quy định.

- Phân công đầu mối phụ trách công tác an toàn thông tin; chịu trách nhiệm quản lý tài khoản, thiết bị, dữ liệu và việc khai thác, sử dụng các hệ thống thông tin thuộc phạm vi quản lý của đơn vị.

- Chủ động kiểm tra, phát hiện, xử lý các nguy cơ mất an toàn thông tin; kịp thời báo cáo Sở đối với sự cố nghiêm trọng hoặc nội dung vượt thẩm quyền.

4. Công chức, viên chức và người lao động thuộc Sở

- Nghiêm túc chấp hành các quy định về an ninh mạng, an toàn thông tin, bảo vệ dữ liệu cá nhân và bí mật nhà nước trong quá trình thực hiện nhiệm vụ.

- Có trách nhiệm bảo vệ tài khoản, mật khẩu, thiết bị được giao; không tự ý cài đặt phần mềm, kết nối thiết bị không bảo đảm an toàn hoặc thực hiện các hành vi có nguy cơ gây mất an toàn thông tin.

- Kịp thời thông báo cho đầu mối phụ trách khi phát hiện dấu hiệu bất thường, nguy cơ mất an toàn thông tin hoặc sự cố liên quan đến hệ thống thông tin, dữ liệu.

Trên đây là Kế hoạch triển khai thực hiện công tác bảo đảm an ninh mạng, an ninh dữ liệu Quý IV năm 2026 của Sở Xây dựng. Yêu cầu Trưởng các phòng, Thủ trưởng các đơn vị trực thuộc và toàn thể công chức, viên chức, người lao động nghiêm túc triển khai thực hiện./.

Nơi nhận
- Công an tỉnh (báo cáo);
- GĐ, các PGĐ Sở;
- Các phòng CMNV Sở;
- Các đơn vị thuộc Sở;
- Lưu: VT, VP(Dũng).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

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

Võ Phiến