UBND TỈNH QUẢNG NGÃI **BAN QLDA ĐTXD CÁC CTGT**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 336 /QĐ-BQL	*Quảng Ngãi, ngày 01 tháng 6 năm 2026*

QUYẾT ĐỊNH
Phê duyệt Phương án Ứng phó sự cố, bảo đảm an toàn thông tin đối với Hệ thống mạng LAN phục vụ công tác chỉ đạo, điều hành trong hoạt động của Ban Quản lý dự án đầu tư xây dựng các công trình Giao thông tỉnh

GIÁM ĐỐC BAN QUẢN LÝ DỰ ÁN ĐẦU TƯ XÂY DỰNG CÁC CÔNG TRÌNH GIAO THÔNG TỈNH QUẢNG NGÃI

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

Căn cứ Luật Giao dịch điện tử ngày 29/11/2005;

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

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Căn cứ Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ Quy định chi tiết một số điều của Luật An ninh mạng;

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; Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông 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 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 từ không gian mạng đến năm 2025, định hướng đến năm 2030;

Căn cứ Công văn số 5609/UBND-KGVX ngày 03/11/2022 của Chủ tịch UBND tỉnh tại về việc triển khai thực hiện Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ;

Theo đề nghị của Văn phòng Ban.

QUYẾT ĐỊNH:

Điều 1. Phê duyệt Phương án Ứng phó sự cố, bảo đảm an toàn thông tin mạng đối với Hệ thống mạng LAN phục vụ công tác chỉ đạo, điều hành trong hoạt động của Ban Quản lý dự án đầu tư xây dựng các công trình Giao thông tỉnh *(có Phương án kèm theo)*.

Điều 2. Các nội dung trong Phương án này là căn cứ để Trưởng các phòng chuyên môn nghiệp vụ thuộc Ban chủ động chỉ đạo, điều hành các hoạt động ứng phó sự cố, bảo đảm an toàn thông tin mạng; hạn chế thấp nhất thiệt hại do sự cố mất an toàn an ninh thông tin gây ra đối với Hệ thống mạng LAN của Ban.

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

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

Nơi nhận:
- Như Điều 4;
- Công an tỉnh;
- Lãnh đạo Ban;
- Trưởng các phòng CMNV;
- Trang thông tin điện tử của Ban;
- Lưu: VT, VP.Tâm.

GIÁM ĐỐC

ỦY BAN NHÂN DÂN TỈNH QUẢNG NGÃI
BAN QUẢN LÝ DỰ ÁN ĐẦU TƯ XÂY DỰNG CÁC CÔNG TRÌNH GIAO THÔNG TỈNH QUẢNG NGÃI

Trần Hoàng Vĩnh

UBND TỈNH QUẢNG NGÃI
BAN QUẢN LÝ DỰ ÁN ĐẦU TƯ XÂY DỰNG CÁC CÔNG TRÌNH GIAO THÔNG TỈNH QUẢNG NGÃI

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

PHƯƠNG ÁN
Ứng phó sự cố, bảo đảm an toàn thông tin đối với Hệ thống mạng LAN phục vụ công tác chỉ đạo, điều hành trong hoạt động của Ban Quản lý dự án đầu tư xây dựng các công trình Giao thông tỉnh

(Kèm theo Quyết định số 336/QĐ-BQL ngày 01/6/2026 của Giám đốc Ban Quản lý dự án đầu tư xây dựng các công trình Giao thông tỉnh)

I. MỤC ĐÍCH, YÊU CẦU

1. Phương án này hướng dẫn việc ứng phó sự cố hệ thống thông tin, trách nhiệm của các phòng chuyên môn nghiệp vụ thuộc Ban và cá nhân có liên quan đến đảm bảo an toàn, an ninh thông tin đối với Hệ thống mạng LAN của Ban Quản lý dự án đầu tư xây dựng các công trình Giao thông tỉnh *(viết tắt là Ban QLDA)*.

2. Thường xuyên quán triệt và thực hiện có hiệu quả phương châm chủ động thực hiện săn lùng mối nguy hại và rà quét lỗ hổng hệ thống thông tin trong phạm vi quản lý nhằm phòng ngừa, chủ động, ứng phó kịp thời, khắc phục khẩn trương và hiệu quả các sự cố xảy ra.

3. Nâng cao năng lực xử lý tình huống sự cố tại chỗ của các phòng chuyên môn nghiệp vụ *(viết tắt là CMNV)* thuộc Ban.

4. Tăng cường thông tin, tuyên truyền, cảnh báo, hướng dẫn các biện pháp phòng, tránh ứng phó sự cố hệ thống thông tin nhằm phát huy ý thức tự giác, chủ động ứng phó của viên chức và người lao động thuộc Ban.

II. NHIỆM VỤ TRỌNG TÂM

1. Trách nhiệm của Văn phòng Ban: Chịu trách nhiệm trước Giám đốc Ban trong việc ứng cứu sự cố an toàn thông tin của Ban, như sau:

- Thực hiện các nhiệm vụ quản lý hệ thống thông tin theo quy định tại Điều 20, Nghị định 85/2016/NĐ-CP.

- Kiểm tra thực hiện, đôn đốc, giám sát công tác đảm an toàn thông tin trong hệ thống thông tin nội bộ tại Ban theo quy định tại Điều 21, Nghị định 85/2016/NĐ-CP.

- Đảm bảo vận hành tốt đối với hệ thống thông tin thuộc phạm vi quản lý.

- Làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trong nội bộ đơn vị.

- Định kỳ tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng LAN theo chỉ đạo của UBND tỉnh hoặc hướng dẫn của Công an tỉnh Quảng Ngãi. Tùy theo mức độ sự cố, phối hợp với Công an tỉnh Quảng Ngãi và các đơn vị có liên quan xử lý, ứng cứu các sự cố an toàn thông tin mạng.

- Tổng hợp và báo cáo về tình hình an toàn thông tin mạng theo định kỳ của Công an tỉnh Quảng Ngãi.

- Hàng năm cử viên chức chuyên trách quản trị mạng tham gia các chương trình đào tạo, tập huấn về công tác bảo đảm an toàn thông tin mạng do Công an tỉnh Quảng Ngãi tổ chức.

- Tham mưu Giám đốc Ban chỉ đạo các phòng CMNV thực hiện nghiêm túc, đảm bảo an toàn, an ninh thông tin; phối hợp với Ban Biên tập Trang thông tin điện tử Ban tuyên truyền, hướng dẫn đến viên chức và người lao động về công tác bảo đảm an toàn thông tin mạng.

- Hàng năm lập dự toán kinh phí cho việc ứng dụng công nghệ thông tin nói chung và công tác bảo đảm an toàn thông tin mạng nói riêng trong nội bộ Ban; lập kế hoạch nâng cấp, bảo trì, sửa chữa, cài đặt phần mềm Phòng chống mã độc... Đề xuất sửa chữa, nâng cấp, thay thế trang thiết bị không phù hợp để đảm bảo an toàn thông tin trong toàn toàn hệ thống.

2. Trách nhiệm của các phòng chuyên CMNV thuộc Ban

- Trưởng các phòng CMNV chỉ đạo viên chức và người lao động của phòng mình thực hiện nghiêm các quy định đảm bảo an toàn thông tin trong toàn hệ thống mạng LAN của Ban, không sử dụng các thiết bị ngoại vi để sao chép, chia sẻ thông tin, dữ liệu.

- Nâng cao ý thức trách nhiệm của viên chức và người lao động thuộc phòng quản lý về đảm bảo an toàn thông tin trong hệ thống mạng LAN của Ban.

- Phối hợp với Văn phòng Ban trong công tác kiểm tra, phát hiện, xử lý kịp thời các sự cố về an toàn thông tin mạng.

3. Trách nhiệm của viên chức và người lao động trong đơn vị

- Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng.

- Tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng; Khai thác, sử dụng có hiệu quả các phần mềm dùng chung của tỉnh.

- Tìm kiếm thông tin trên mạng từ các trang chính thống và tìm kiếm văn bản liên quan đến công tác tham mưu tại Cổng Thông tin điện tử UBND tỉnh và Trang Thông tin điện tử Ban.

- Phối hợp với viên chức quản trị mạng của Ban trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn thông tin mạng

III. BIỆN PHÁP THỰC HIỆN

1. Biện pháp phòng ngừa sự cố hệ thống thông tin

1.1. Về thông tin, tuyên truyền

- Trưởng các phòng CMNV thuộc Ban tăng cường công tác tuyên truyền đến viên chức và người lao động nhằm nâng cao ý thức trách nhiệm về đảm bảo an toàn thông tin trong hệ thống mạng LAN.

- Nội dung tuyên truyền về an toàn, an ninh thông tin, gồm những điểm cơ bản, như sau:

+ Hệ thống thông tin là tập hợp các thiết bị viễn thông, công nghệ thông tin bao gồm phần cứng, phần mềm và cơ sở dữ liệu phục vụ cho hoạt động lưu trữ, xử lý, truyền đưa, chia sẻ, trao đổi, cung cấp và sử dụng thông tin.

+ An toàn thông tin là sự bảo vệ thông tin và các hệ thống thông tin tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

+ An ninh thông tin là việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

+ Phần mềm độc hại là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

+ Người dùng: Viên chức và người lao động tại các phòng CMNV thuộc Ban sử dụng máy tính, các thiết bị điện tử để xử lý công việc.

+ Tham số mạng: Là các tham số kỹ thuật được cài đặt trong các thiết bị mạng và thiết bị máy tính để tạo ra các địa chỉ kết nối trong mạng. Các máy tính gửi và nhận thông tin thông qua các địa chỉ kết nối này.

+ Tính toàn vẹn: Bảo vệ tính chính xác và tính đầy đủ của thông tin và các phương pháp xử lý thông tin.

+ Tính tin cậy: Đảm bảo thông tin chỉ có thể được truy cập bởi những người được cấp quyền sử dụng.

+ Tính sẵn sàng: Đảm bảo những người được cấp quyền có thể truy cập thông tin và các tài nguyên (mạng, máy chủ, tên miền, tài khoản thư điện tử…) ngay khi có nhu cầu.

+ Sự cố an toàn thông tin mạng (sau đây gọi tắt là sự cố) là việc thông tin, hệ thống thông tin bị tấn công hoặc gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng. Sự cố có thể là sự kiện đã, đang hoặc có khả năng xảy ra gây mất an toàn thông tin trên môi trường mạng (LAN, WAN, INTERNET…), được phát hiện thông qua việc giám sát, đánh giá, phân tích của các cơ quan, tổ chức, cá nhân có liên quan hoặc được cảnh báo từ các chuyên gia, tổ chức về lĩnh vực an toàn thông tin trong nước và trên thế giới.

+ Sự cố có tính chất nghiêm trọng là sự cố có một hoặc nhiều tính chất sau: Có khả năng xảy ra trên diện rộng, lan nhanh; có khả năng phá hoại hệ thống mạng máy tính; lấy cắp dữ liệu, có thể gây thiệt hại lớn cho các hệ thống thông

tin quan trọng như: Cổng thông tin điện tử, Cổng dịch vụ công và hệ thống thông tin một cửa điện tử, hệ thống quản lý văn bản và điều hành, hệ thống thư điện tử công vụ… và các hệ thống thông tin, cơ sở dữ liệu chuyên ngành của Ban, đòi hỏi sự tham gia phối hợp của nhiều cơ quan, đơn vị trong tỉnh và cần có sự hỗ trợ của các cơ quan, đơn vị chuyên trách quốc gia để giải quyết.

+ Ứng phó sự cố là hoạt động nhằm xử lý, khắc phục sự cố gây mất an toàn thông tin mạng gồm: Theo dõi, thu thập, phân tích, phát hiện, cảnh báo, điều tra, xác minh sự cố, ngăn chặn sự cố, khôi phục dữ liệu và khôi phục hoạt động bình thường của hệ thống thông tin.

+ Tuyên truyền, phổ biến các văn bản, quy định hiện hành về an toàn an ninh thông tin, như: Luật An toàn thông tin mạng, Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 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; 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; Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông 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; Quyết định số 03/2019/QĐ-UBND ngày 21/12/2019 của UBND tỉnh Quảng Ngãi về việc ban hành Quy định về đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Quảng Ngãi; Kế hoạch số 166/KH-UBND ngày 14/10/2022 của UBND tỉnh về tăng cường đảm bảo an toàn, an ninh thông tin trong hoạt động các cơ quan nhà nước tỉnh Quảng Ngãi đến năm 2025 và định hướng đến năm 2030 và các văn bản quy phạm pháp luật về an toàn thông tin mạng và các văn bản quy phạm pháp luật, tài liệu hướng dẫn chuyên môn về an toàn thông tin mạng.

1.2. Nhận diện các nguy cơ, sự cố hệ thống thông tin

Các nguy cơ, sự cố có khả năng ảnh hưởng đến hệ thống thông tin đối với Hệ thống mạng LAN của Ban, như sau:

1.2.1 Sự cố do bị tấn công mạng:

- 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 từ chối dịch vụ;
- Tấn công giả mạo;
- 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.

1.2.2 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;

1.2.3 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 an toàn thông tin;

- 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.

1.2.4 Sự cố liên quan đến các thảm họa tự nhiên: Bão, lụt, động đất, hỏa hoạn,...

1.3. Phòng chống virus máy tính, bảo mật cơ sở dữ liệu và an ninh mạng

a) Bảo mật số liệu: Viên chức và người lao động tại các phòng CMNV thuộc Ban phải có trách nhiệm bảo mật số liệu nghiệp vụ trên máy tính. Tuyệt đối không chia sẽ thư mục, dữ liệu cá nhân trên hệ thống mạng LAN của Ban.

b) Bảo mật truy cập: Các chương trình, phần mềm được bàn giao cho viên chức và người lao động sử dụng phải được thiết lập mật khẩu theo quy định. Kịp thời điều chỉnh vị trí công tác cho người sử dụng (khi có sự thay đổi); xóa khỏi hệ thống các tài khoản người dùng đã về hưu hoặc chuyển công tác.

c) Bảo mật hệ thống mạng và truyền tin: Mạng và đường truyền được áp dụng các chế độ bảo mật cần thiết, chống xâm nhập bất hợp pháp. Viên chức quản trị mạng có trách nhiệm thường xuyên theo dõi, kiểm tra phát hiện kịp thời các hoạt động xâm nhập và có biện pháp xử lý kịp thời.

d) An toàn trong sử dụng: Khi không làm việc với máy vi tính trong thời gian dài, viên chức và người lao động tại các phòng CMNV thuộc Ban phải tắt máy tính hoặc đặt chế độ bảo vệ để đảm bảo an toàn cho dữ liệu của cá nhân.

e) Phòng, chống virus: Viên chức và người lao động tại các phòng CMNV thuộc Ban có trách nhiệm tuân thủ các biện pháp, tài liệu hướng dẫn về cảnh báo về lỗ hổng bảo, cảnh báo nguy cơ tấn công theo tài liệu hướng dẫn của cơ quan có thẩm quyền nhằm rà soát, giám sát, ngăn chặn, phòng ngừa, xử lý kịp thời hạn chế đến mức thấp nhất nguy cơ gây mất an toàn an ninh thông tin. Mọi dữ liệu từ các thiết bị lưu trữ bên ngoài (USB, ổ cứng di động, thẻ nhớ…) đều phải được quét, diệt virus trước khi sao chép vào máy. Những máy tính phát hiện có virus, nguy cơ bị tấn công phải báo ngay cho viên chức quản trị mạng và tách

khỏi mạng về mặt vật lý để tránh tình trạng lây nhiễm sang các máy tính khác. Không truy cập vào các trang website, đường dẫn liên kết không rõ ràng; không truy cập vào các link hoặc tải về các file tài liệu từ các địa chỉ thư không nắm rõ thông tin, địa chỉ người gửi.

1.4. Kiểm soát việc cài đặt các phần mềm và thực hiện cơ chế sao lưu, phục hồi

a) Kiểm soát chặt chẽ việc cài đặt các phần mềm mới lên máy chủ, máy trạm

Các phần mềm được cài đặt trên các máy trạm (*bao gồm hệ điều hành, các phần mềm ứng dụng văn phòng, phần mềm phục vụ công việc, tiện ích khác)* phải được thường xuyên theo dõi, cập nhật bản vá lỗi bảo mật của nhà phát triển, lựa chọn cài đặt các phần mềm chống, diệt virus, mã độc và thường xuyên cập nhật phiên bản mới, đặt lịch quét virus theo định kỳ.

b) Cơ chế sao lưu, phục hồi máy chủ, máy trạm

Viên chức và người lao động phải thực hiện việc sao lưu định kỳ cơ sở dữ liệu và các dữ liệu quan trọng khác (bao gồm dữ liệu phát sinh trong quá trình vận hành các phần mềm ứng dụng như: các tập tin văn bản, hình ảnh,..) vào các thiết bị lưu trữ bên ngoài (USB, ổ cứng di động, thẻ nhớ...) nhằm phục vụ cho việc phục hồi, khắc phục dữ liệu kịp thời khi có sự cố xảy ra.

1.5. Đảm bảo an toàn hệ thống thông tin mạng LAN

a) Về cơ sở hạ tầng: Đảm bảo việc lắp đặt thiết bị chống sét, thiết bị cảnh báo phòng chống cháy, nổ tại trụ sở để bảo vệ hệ thống, thiết bị công nghệ thông tin.

b) Quản lý hệ thống mạng nội bộ: Mạng nội bộ của Ban khi kết nối với mạng Internet phải thông qua thiết bị tường lửa, để kiểm soát, hạn chế việc truy cập trái phép từ bên ngoài. Các máy chủ, máy trạm trên hệ thống phải được cài đặt phần mềm diệt virus có bản quyền.

c) Quản lý hệ thống mạng không dây (Wifi): Khi thiết lập mạng không dây có kết nối vào mạng nội bộ được cấu hình và quản lý thông qua thiết bị tường lửa nhằm kiểm soát truy cập, giám sát lưu lượng và bảo đảm an toàn thông tin. Việc triển khai mạng không dây thực hiện các biện pháp bảo mật như thiết lập định danh mạng (SSID), xác thực truy cập bằng mật khẩu, áp dụng cơ chế mã hóa dữ liệu, phân tách vùng mạng phù hợp và thay đổi mật khẩu định kỳ.

d) Quản lý truy cập từ xa vào mạng nội bộ: Đối với việc truy cập từ xa vào mạng nội bộ phải được theo dõi, quản lý chặt chẽ, nhất là truy cập có sử dụng chức năng quản trị, phải thiết lập mật mã độ an toàn cao, thường xuyên thay đổi mật mã, hạn chế truy cập từ xa vào mạng nội bộ từ các điểm truy cập Internet công cộng.

IV. PHÂN CÔNG THỰC HIỆN

1. Trách nhiệm của Trưởng các phòng CMNV thuộc Ban

- Thường xuyên chỉ đạo viên chức và người lao động của phòng thực hiện nghiêm các quy định bảo đảm an toàn thông tin hệ thống mạng LAN của Ban.

- Phối hợp với Văn phòng Ban trong công tác kiểm tra, phát hiện, xử lý kịp thời các sự cố về an toàn thông tin mạng.

2. Trách nhiệm của viên chức và người lao động tại các phòng CMNV thuộc Ban

- Có trách nhiệm quản lý tài khoản, mật khẩu đăng nhập vào các phần mềm dùng chung được triển khai tại Ban; thực hiện nghiêm các quy định về đảm bảo an toàn thông tin trong hệ thống mạng LAN của Ban. Thường xuyên thay đổi mật khẩu đủ mạnh (ít nhất 8 ký tự, có chữ hoa, chữ thường, số, ký tự đặc biệt) để đảm bảo an toàn, an ninh thông tin.

- Tự quản lý, bảo quản thiết bị công nghệ thông tin như: Máy tính, máy in, máy scan, máy photocopy... mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp thiết bị.

- Thực hiện tiếp nhận, xử lý, phát hành, quản lý và lưu trữ văn bản, hồ sơ điện tử trên phần mềm quản lý văn bản đúng quy định trên môi trường mạng và ký số cá nhân, đảm bảo theo đúng quy định pháp luật hiện hành. Không sử dụng gmail, yahoo… để gửi, nhận văn bản giữa các cơ quan nhà nước.

- Không được tự ý cài đặt phần mềm không rõ nguồn gốc trên mạng hoặc gỡ bỏ phần mềm diệt vius đã được cài đặt trên máy trạm.

- Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm virus, nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm diệt virus, mất dữ liệu,…), người sử dụng phải báo ngay cho quản trị mạng đơn vị để phối hợp xử lý kịp thời tránh lây lan đến các máy trạm khác.

3. Trách nhiệm của viên chức quản trị mạng của Ban

- Làm đầu mối ứng cứu sự cố đối với hệ thống mạng LAN của Ban theo đúng quy trình ứng cứu sự cố dựa trên tính chất, mức độ, phạm vi và nguyên nhân xảy ra sự cố; bảo đảm nhanh chóng, chính xác, kịp thời, an toàn và hiệu quả.

- Phối hợp với các cơ quan, đơn vị có liên quan kiểm tra, rà soát đánh giá an toàn thông tin thường xuyên, định kỳ hoặc đột xuất khi có các yếu tố quan trọng, đặc biệt thay đổi để kịp thời phát hiện các lỗ hổng đang tồn tại, các nguy cơ mất an toàn thông tin mạng.

- Tham mưu trình Giám đốc Ban các văn bản tuyên truyền, phổ biến nâng cao nhận thức về an toàn thông tin tại Ban.

- Thực hiện phân quyền truy cập và hướng dẫn sử dụng cho viên chức và người lao động tại Ban ứng dụng các phần mềm dùng chung của tỉnh đang triển khai tại Ban (như Phần mềm Quản lý văn bản và điều hành - iOffice; Hệ thống thông tin giải quyết thủ tục hành chính tỉnh Quảng Ngãi; Hệ thống thông tin báo cáo Bộ, ngành, địa phương...); kịp thời điều chỉnh vị trí công tác cho người sử

dụng (khi có sự thay đổi); xóa khỏi hệ thống các tài khoản người dùng đã nghỉ hưu hoặc chuyển công tác.

- Chịu trách nhiệm quản lý các tài khoản quản trị được bàn giao và thường xuyên thay đổi mật khẩu quản trị đủ mạnh để đảm bảo an toàn, bảo mật thông tin. Mật khẩu có ít nhất 8 ký tự, có chữ hoa, chữ thường, số, ký tự đặc biệt, tránh nguy cơ mất an toàn an ninh thông tin.

- Chủ động thực hiện lùng ra các mối nguy hại và rà quét lỗ hổng hệ thống thông tin trong phạm vi quản lý tối thiểu 01 lần/6 tháng.

- Tham mưu trình Giám đốc Ban các văn bản gửi Cục Chứng thực số và Bảo mật thông tin, Ban Cơ yếu Chính phủ cấp mới, thu hồi, gia hạn chứng thư số đơn vị, cá nhân theo đúng quy định tại Nghị định số 130/NĐ-CP ngày 27/9/2018 của Chính phủ quy định chi tiết thi hành Luật giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số; Thông tư số 185/2019/TT-BQP ngày 04/12/2019 của Bộ trưởng Bộ Quốc phòng Hướng dẫn việc cung cấp, quản lý, sử dụng dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ.

- Tham mưu trình Giám đốc Ban việc sửa chữa, bảo trì, cài đặt các thiết bị, phần mềm bảo mật cho các máy tính các phòng CMNV thuộc Ban tránh nguy cơ mất an toàn, an ninh thông tin máy trạm người dùng.

- Tham mưu trình Giám đốc Ban cử viên chức và người lao động tại Ban tham dự các lớp kỹ năng bảo vệ hệ thống thông tin do Công an tỉnh Quảng Ngãi và các cơ quan có liên quan tổ chức.

4. Phương án ứng phó sự cố an toàn hệ thống thông tin

Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm virus, nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm diệt virus, mất dữ liệu,…), viên chức và người lao động tại các phòng CMNV thuộc Ban thực hiện các bước như sau:

+ Bước 1. Khoanh vùng cô lập sự cố

- Sau khi phát hiện sự cố, viên chức và người lao động tại các phòng CMNV thực hiện khoanh vùng cô lập máy tính bị sự cố, như: ngắt kết nối máy tính khỏi hệ thống thông tin mạng LAN của Ban (tắt máy, rút dây mạng…).

- Báo cáo ngay Lãnh đạo phòng các dấu hiệu sự cố; đồng thời thông báo kịp thời về Văn phòng Ban để cử viên chức Quản trị mạng phối hợp kiểm tra, xử lý.

+ Bước 2. Thu thập thông tin phục vụ phân tích sự cố

- Viên chức quản trị mạng Ban phối hợp với viên chức và người lao động tại phòng CMNV thuộc Ban kiểm tra máy tính đang bị sự cố để nắm bắt thông tin ban đầu về sự cố.

- Các thông tin thu thập gồm: Thông tin hệ thống; chức năng của hệ thống; cấu hình của hệ thống (OS, servise, version, network,…); Thu thập chứng cứ; Thu thập bộ nhớ; Thu thập trạng thái network và các kết nối; Thu thập các

tiến trình đang chạy; Thu thập hard drive media; Thu thập removeble media; Thu thập Log file…).

+ Bước 3. Phân tích sự cố

- Viên chức quản trị mạng Ban phối hợp với viên chức và người lao động tại phòng CMNV thuộc Ban kiểm tra máy tính đang bị sự cố để phân tích nguyên nhân ban đầu về sự cố.

- Các thông tin phân tích gồm: Phân tích dòng thời gian; Thời gian bị sửa đổi, truy cập, tạo hoặc thay đổi; Thời gian thực hiện các cập nhật lớn đối với hệ thống; Thời điểm mà hệ thống sử dụng lần cuối cùng; Phân tích dữ liệu; Kiểm tra sự thay đổi cấu hình; Kiểm tra hệ thống tập tin có bị mã độc; Kiểm tra tập tin Internet history và các tập tin history khác; Kiểm tra Registry và tiến trình; Quan sát các tập tin, tiến trình lúc khởi động; Phân tích log file.

+ Bước 4. Xử lý sự cố

- Trường hợp sự cố có khả năng kiểm soát, xử lý được: Viên chức quản trị mạng của Ban tiến hành xử lý sự cố bao gồm các bước: Gỡ bỏ sự cố; Xác định và gỡ bỏ các backdoors; Phân tích và kiểm tra lỗ hỗng sau khi thực hiện các bản vá lỗi; Khôi phục dữ liệu; Thu thập các tập tin, hình ảnh, email, … bị xóa, thời gian bị xóa; Tìm kiếm các tập tin không thể khôi phục; Khôi phục các tập tin phù hợp.

- Trường hợp sự cố ngoài khả năng kiểm soát, xử lý được (sự cố có tính chất nghiêm trọng): Triển khai ngay các biện pháp xử lý ngăn chặn tấn công tránh lây nhiễm sự cố các máy tính khác trên hệ thống thông tin và báo cáo về Văn phòng Ban đề xuất Giám đốc Ban có văn bản đề nghị Công an tỉnh Quảng Ngãi, Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi có các biện pháp hỗ trợ, xử lý kịp thời.

+ Bước 5. Tổng hợp báo cáo

- Sau khi triển khai các giải pháp ứng cứu sự cố, viên chức quản trị mạng Ban tham mưu trình Giám đốc Ban tổ chức họp phân tích nguyên nhân, rút kinh nghiệm trong hoạt động xử lý sự cố và đề xuất các biện pháp ứng cứu cho các sự cố tương tự.

- Tham mưu Giám đốc Ban gửi báo cáo kết quả ứng cứu sự cố xảy ra về Công an tỉnh Quảng Ngãi, Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi để biết, theo dõi.

+ Bước 6. Lưu hồ sơ

Toàn bộ các hồ sơ trong quá trình xử lý sự cố, viên chức quản trị mạng Ban lưu trữ phục vụ các hoạt động quản lý và theo dõi, kiểm tra định kỳ.

V. TỔ CHỨC THỰC HIỆN

1. Công tác phòng ngừa, ứng phó sự cố hệ thống thông tin là nhiệm vụ đặc biệt quan trọng, là trách nhiệm chung của toàn thể viên chức và người lao động tại Ban; để chủ động phòng, ngừa, ứng phó kịp thời và khắc phục sớm hậu

quả do sự cố gây ra, hạn chế đến mức thấp nhất thiệt hại về dữ liệu thông tin, tài sản của Ban QLDA. Do đó, từng phòng CMNV thuộc Ban cần nổ lực tổ chức phối hợp đồng bộ nhằm đưa công tác phòng ngừa, ứng phó sự cố an ninh thông tin hiệu quả; Tổ chức tìm kiếm các mối nguy hại và rà quét lỗ hổng hệ thống thông tin trong phạm vi quản lý theo quy định.

2. Các phòng CMNV thuộc Ban trong phạm vi nhiệm vụ, quyền hạn của mình, có trách nhiệm phối hợp với Văn phòng Ban trong quá trình tham gia ứng cứu sự cố an toàn thông tin khi xảy ra sự cố.

3. Viên chức quản trị mạng Xây dựng hồ sơ đề xuất cấp độ an toàn hệ thống thông tin đối với các hệ thống thông tin của đơn vị mình theo quy định; gửi về Công an tỉnh Quảng Ngãi thẩm định phê duyệt. Căn cứ Phương án này, ban hành Phương án Ứng phó sự cố, bảo đảm an toàn thông tin đối với Hệ thống thông tin của đơn vị để triển khai thực hiện.

4. Phương án này được phổ biến đến toàn thể viên chức và người lao động thuộc Ban biết để thực hiện. Trong quá trình thực hiện nếu có vướng mắc và cần sửa đổi, bổ sung, đề nghị các phòng CMNV, cá nhân kịp thời phản ánh về Văn phòng Ban để tổng hợp báo cáo Giám đốc Ban xem xét, sửa đổi, bổ sung cho phù hợp./.