ỦY BAN NHÂN DÂN PHƯỜNG ĐẠI YÊN	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 293/QĐ-UBND	*Đại Yên, ngày 14 tháng 11 năm 2024*

QUYẾT ĐỊNH
Về việc ban hành phương án ứng cứu, xử lý sự cố cho hệ thống thông tin của UBND phường Đại Yên

CHỦ TỊCH ỦY BAN NHÂN DÂN PHƯỜNG ĐẠI YÊN

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19/6/2015;Căn cứ Luật sửa đổi, bổ sung một số điều của Luật Tổ chức Chính phủ và Luật Tổ chức chính quyền địa phương ngày 22/11/2019

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

Căn cứ các 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 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 xử lý sự cố an toàn thông tin mạng Việt Nam;

Căn cứ Chỉ thị 09/CT-TTg ngày 23/02/2024 của Thủ tướng Chính phủ về tuân thủ quy định pháp luật về tăng cường 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 quy định về điều phối, ứng cứu xử lý sự cố an toàn thông tin mạng trên toàn quốc;

Theo đề nghị của công chức Văn phòng – Thống kê.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Phương án ứng cứu, xử lý sự cố cho hệ thống thông tin của UBND phường Đại Yên, thành phố Hạ Long, tỉnh Quảng Ninh.

Điều 2. Quyết định này có hiệu lực từ ngày ký.

Điều 3. Cán bộ, công chức, người lao động và cá nhân có liên quan trực tiếp đến hệ thống thông tin của UBND phường Đại Yên chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như điều 3
- UBND thành phố (B/cáo);
- Lưu: VP.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

U.B.N.D PHƯỜNG ĐẠI YÊN TP. HẠ LONG T. QUẢNG NINH

Nguyễn Văn Mạnh

PHƯƠNG ÁN, QUY TRÌNH ỨNG CỨU XỬ LÝ SỰ CỐ CHO HỆ THỐNG THÔNG TIN

(Ban hành kèm theo Quyết định số 293/QĐ-UBND ngày 14/11/2024 của Ủy ban nhân dân phường Đại Yên)

CHƯƠNG I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Phạm vi điều chỉnh: Quy định này áp dụng cho các phương án ứng cứu, xử lý sự cố xảy ra đối với hệ thống thông tin sử dụng trong hoạt động của cơ quan phường Đại Yên, nhằm đảm bảo an toàn và duy trì sự liên tục của hệ thống thông tin, phục vụ các hoạt động quản lý, điều hành và giao dịch của phường.

2. Đối tượng áp dụng:

- Cán bộ, công chức, người lao động và cá nhân có liên quan trực tiếp đến hệ thống thông tin của UBND phường Đại Yên.

Điều 2. Giải thích từ ngữ

1. Sự cố an toàn thông tin mạng 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 (sau đây gọi tắt là sự cố).

Sự cố an toàn thông tin mạng nghiêm trọng là sự cố đáp ứng đồng thời các tiêu chí sau:

- Hệ thống thông tin bị sự cố là hệ thống thông tin cấp độ 4, cấp độ 5 hoặc thuộc Danh mục hệ thống thông tin quan trọng quốc gia và bị một trong số các sự cố sau: Hệ thống bị gián đoạn dịch vụ; Dữ liệu tuyệt mật hoặc bí mật nhà nước có khả năng bị tiết lộ; Dữ liệu quan trọng của hệ thống không bảo đảm tính toàn vẹn và không có khả năng khôi phục được; Hệ thống bị mất quyền điều khiển; Sự cố có khả năng xảy ra trên diện rộng hoặc gây ra các ảnh hưởng dây chuyền, làm tổn hại cho các hệ thống thông tin cấp độ 4 hoặc cấp độ 5 khác.

- Chủ quản hệ thống thông tin không đủ khả năng tự kiểm soát, xử lý được sự cố.

2. Ứng cứu xử lý sự cố an toàn thông tin mạng 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.

Điều 3. Phân công tổ chức thực hiện ứng cứu xử lý sự cố cho hệ thống thông tin

1) Bộ phận ứng cứu, xử lý sự cố (Bộ phận Văn phòng – Thống kê), chủ trì ứng cứu xử lý sự cố ATTT mạng của phường Đại Yên có trách nhiệm tham gia

hoạt động ứng cứu khẩn cấp đảm bảo ATTT mạng nội bộ khi có yêu cầu từ các bộ phận, cá nhân của đơn vị.

2) Các bộ phận, cá nhân của phường Đại Yên có trách nhiệm phối hợp cùng tham gia hoạt động ứng cứu khẩn cấp đảm bảo ATTT mạng nội bộ đảm bảo đạt hiệu quả

Điều 4. Nguyên tắc điều phối, ứng cứu xử lý sự cố

1. Tuân thủ các quy định pháp luật về điều phối, ứng cứu xử lý sự cố an toàn thông tin mạng.

2. Chủ động, kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả.

3. Phối hợp chặt chẽ, chính xác, đồng bộ và hiệu quả giữa các bộ phận.

4. Ứng cứu xử lý 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.

CHƯƠNG II

ĐÁNH GIÁ CÁC NGUY CƠ, SỰ CỐ AN TOÀN HỆ THỐNG THÔNG TIN

Điều 5. Đánh giá các nguy cơ, sự cố hệ thống thông tin:

1. Đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng của các hệ thống thông tin và các đối tượng cần bảo vệ.

2. 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 được bảo vệ.

3. Đánh giá, dự báo các hậu quả, thiệt hại, tác động có thể nếu xảy ra sự cố.

4. Đánh giá về hiện trạng phương tiện, trang thiết bị, công cụ hỗ trợ, nhân lực phục vụ đối phó, ứng cứu, khắc phục sự cố.

5. Các nguy cơ mất an toàn thông tin

- Nguy cơ mất an toàn thông tin về khía cạnh vật lý:

Nguy cơ mất an toàn thông tin về khía cạnh vật lý là nguy cơ do mất điện, nhiệt độ, độ ẩm không đảm bảo, hỏa hoạn, thiên tai, thiết bị phần cứng bị hư hỏng, phá hoại.

- Nguy cơ bị mất, hỏng, sửa đổi nội dung thông tin:

Người dùng có thể vô tình để lộ mật khẩu hoặc không thao tác đúng quy trình tạo cơ hội cho kẻ xấu lợi dụng để lấy cắp hoặc làm hỏng thông tin.

Kẻ xấu có thể sử dụng công cụ hoặc kỹ thuật của mình để thay đổi nội dung thông tin (các file) nhằm sai lệnh thông tin của chủ sở hữu hợp pháp.

- Nguy cơ bị tấn công bởi các phần mềm độc hại:

Các phần mềm độc hại tấn công bằng nhiều phương pháp khác nhau để xâm nhập vào hệ thống với các mục đích khác nhau như: virus, sâu máy tính (Worm), phần mềm gián điệp (Spyware),...

- Nguy cơ xâm nhập từ lỗ hổng bảo mật:

Lỗ hổng bảo mật thường là do lỗi lập trình, lỗi hoặc sự cố phần mềm, nằm trong một hoặc nhiều thành phần tạo nên hệ điều hành hoặc trong chương trình cài đặt trên máy tính.

- Nguy cơ xâm nhập do bị tấn công bằng cách phá mật khẩu:

Quá trình truy cập vào một hệ điều hành có thể được bảo vệ bằng một khoản mục người dùng và một mật khẩu. Đôi khi người dùng khoản mục lại làm mất đi mục đích bảo vệ của nó bằng cách chia sẻ mật khẩu với những người khác, ghi mật khẩu ra và để nó công khai hoặc để ở một nơi nào đó cho dễ tìm trong khu vực làm việc của mình.

- Nguy cơ mất an toàn thông tin do sử dụng e-mail:

Tấn công có chủ đích bằng thư điện tử là tấn công bằng thư điện tử giả mạo giống như thư điện tử được gửi từ người quen, có thể gắn tập tin đính kèm nhằm làm cho thiết bị bị nhiễm virus. Cách thức tấn công này thường nhằm vào một cá nhân hay một tổ chức cụ thể. Thư điện tử đính kèm tập tin chứa virus được gửi từ kẻ mạo danh là một đồng nghiệp hoặc một đối tác nào đó. Người dùng bị tấn công bằng thư điện tử có thể bị đánh cắp mật khẩu hoặc bị lây nhiễm virus. Ngoài ra, e-mail cũng có thể chứa một liên kết tới một web site giả.

- Nguy cơ mất an toàn thông tin trong quá trình truyền tin:

Trong quá trình lưu thông và giao dịch thông tin trên mạng internet nguy cơ mất an toàn thông tin trong quá trình truyền tin là rất cao do kẻ xấu chặn đường truyền và thay đổi hoặc phá hỏng nội dung thông tin rồi gửi tiếp tục đến người nhận.

CHƯƠNG III

PHƯƠNG ÁN ĐỐI PHÓ, ỨNG CỨU XỬ LÝ SỰ CỐ AN TOÀN THÔNG TIN MẠNG

Điều 6. Phân nhóm sự cố an toàn thông tin mạng

1. Sự cố an toàn thông tin mạng nghiêm trọng là sự cố đáp ứng đồng thời các tiêu chí sau:

a) Hệ thống thông tin bị sự cố là hệ thống thông tin của phường Đại Yên bị một trong số các sự cố sau: Dữ liệu quan trọng của hệ thống không bảo đảm tính toàn vẹn và không có khả năng khôi phục được; Hệ thống bị mất quyền điều khiển; Sự cố có khả năng xảy ra trên diện rộng hoặc gây ra các ảnh hưởng dây chuyền, làm tổn hại cho các hệ thống thông tin; ...

b) Chủ quản hệ thống thông tin không đủ khả năng tự kiểm soát, xử lý được sự cố.

2. Sự cố an toàn thông tin thường gặp:

a) Sự cố do bị tấn công mạng: Tấn công từ chối dịch vụ; tấn công giả

mạo; sự cố về tấn công thay đổi giao diện; tấn công sử dụng mã độc; tấn công truy cập trái phép, chiếm quyền điều khiển; tấn công mã hóa phần mềm, dữ liệu, thiết bị; tấn công phá hoại thông tin, dữ liệu, phần mềm; tấn công gián điệp, lấy cắp thông tin, dữ liệu; tấn công trong hợp sử dụng kết hợp nhiều hình thức; các hình thức tấn công mạng khác.

b) Sự cố do lỗi hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc do lỗi đường truyền, hosting,...: Sự cố nguồn điện; sự cố đường kết nối mạng 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.

c) Sự cố do lỗi thao tác 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.

Điều 7. Nguyên tắc, phương châm ứng phó, xử lý sự cố

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

a) Bảo mật dữ liệu: Công chức, viên chức và người lao động phải có trách nhiệm bảo mật số liệu nghiệp vụ trên máy tính.Việc chia sẻ dữ liệu trên mạng do bộ phận quản trị mạng thực hiện theo quyết định của Chủ tịch UBND phường và theo phân cấp sử dụng tài nguyên mạng.

b) Bảo mật truy cập: Các chương trình ứng dụng, phân chia sử dụng trên máy tính phải được đặt mật khẩu, mã khoá bảo mật.

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. Bộ phận, người 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, công chức và người lao động thuộc phường Đại Yên 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: Cán bộ, Công chức, và người lao động thuộc phường Đại Yên có trách nhiệm tuân thủ các biện pháp phòng và chống virus cho máy tính, đảm bảo an toàn dữ liệu thuộc cá nhân quản lý. Mọi dữ liệu từ các thiết bị lưu trữ bên ngoài đều phải được quét, diệt virus mỗi khi đưa vào máy. Những máy tính phát hiện có virus phải được tách khỏi mạng về mặt vật lý để tránh tình trạng lây nhiễm sang các máy tính khác. Không truy cập vào các link liên kết không rõ ràng; không click vào các link, tải về các file tài liệu từ các địa chỉ thư không nắm rõ thông tin, địa chỉ người gửi.

2. Đảm bảo an toàn máy chủ, máy trạm và 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 máy chủ, 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: Công chức, viên chức và người lao động phải 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,..). Sau khi sao lưu, lưu trữ bản sao lưu bằng thiết bị lưu trữ ngoài theo quy định lưu trữ hiện hành nhằm phục vụ cho việc phục hồi, khắc phục hệ thống kịp thời khi có sự cố xảy ra.

3. Đảm bảo an toàn hệ thống mạng máy tính, kết nối Internet

a) Quản lý hệ thống mạng nội bộ: Mạng nội bộ của phường Đại Yên phải được tổ chức theo mô hình Clients/Server; mạng nội bộ khi kết nối với mạng Internet phải thông qua thiết bị tường lửa kiểm soát, có phân chia hệ thống mạng nội bộ thành các vùng mạng theo phạm vi truy cập, vô hiệu hóa tất cả các dịch vụ không sử dụng tại từng vùng mạng, thực hiện nguyên tắc chỉ mở các dịch vụ cần thiết khi có yêu cầu.

b) Quản lý hệ thống mạng không dây (wifi): Khi thiết lập mạng không dây có kết nối vào mạng nội bộ phải thiết lập các thông số cần thiết như định danh, mật mã, mã hóa dữ liệu, có thay đổi mật mã định kỳ.

c) 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.

4. Đảm bảo an toàn truy cập, đăng nhập hệ thống thông tin

a) Trách nhiệm, quyền hạn người dùng khi truy cập, đăng nhập các hệ thống thông tin, đảm bảo mỗi người dùng khi sử dụng hệ thống thông tin phải được cấp và sử dụng tài khoản truy cập với định danh duy nhất gắn với người dùng đó. Trường hợp sử dụng tài khoản dùng chung cho một nhóm người hay một đơn vị, bộ phận phải có cơ chế xác định các cá nhân có trách nhiệm quản lý tài khoản. Người dùng chỉ được truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình và có trách nhiệm bảo mật tài khoản truy cập được cấp.

b) Mật mã đăng nhập, truy cập hệ thống thông tin phải có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặcbiệt như !, @, #, $, %,...).

5. Đảm bảo an toàn thông tin, dữ liệu

a) Thông tin, dữ liệu khi được lưu trữ, khai thác, trao đổi phải được đảm bảo tính toàn vẹn, tính tin cậy, tính sẵn sàng. Thông tin, dữ liệu quan trọng khi được lưu trữ, trao đổi phải áp dụng kỹ thuật mã hóa, thiết lập mật mã, ứng dụng chữ ký số và phải có cơ chế lưu trữ dự phòng.

b) Trong trao đổi thông tin, dữ liệu phục vụ công việc, cơ quan, công chức, viên chức và người lao động phải sử dụng Hộp thư công vụ điện tử do UBND tỉnh cấp (@quangninh.gov.vn), phần mềm quản lý văn bản và hồ sơ công việc, phần mềm một cửa điện tử. Hạn chế việc sử dụng các phương tiện trao đổi thông tin dữ liệu, hệ thống thư điện tử công cộng, mạng xã hội trên Internet trong hoạt động của Phường Đại Yên Triển khai và tổ chức thực hiện đảm bảo theo các quy định tại quy chế đảm bảo an toàn thông tin mạng của phường Đại Yên Thuê dịch vụ giám sát an toàn thông tin mạng.

Điều 8. Quy trình ứng cứu xử lý sự cố an toàn thông tin mạng

Bước 1: Thông báo sự cố

Cán bộ công chức, viên chức, người lao động tại các phòng, đơn vị, bộ phận thuộc phường Đại Yên, khi gặp sự cố trong quá trình sử dụng máy tính có kết nối mạng thực hiện thông báo ngay cho Bộ phận ứng cứu xử lý sự cố.

Bước 2: Tiếp nhận sự cố

Bộ phận ứng cứu xử lý sự cố tiếp nhận thông tin về sự cố qua các phương thức: điện thoại, trực tiếp,...

Bước 3: Xác minh/xác nhận sự cố

Bộ phận ứng cứu xử lý sự cố triển khai tiến hành xác nhận sự cố bao gồm các thông tin như sau:

- Tình trạng (Sự cố sẽ xảy ra; Sự cố đang xảy ra; Sự cố đã xảy ra);
- Mức độ (Sự cố nghiêm trọng; Sự cố bình thường);
- Phạm vi (Sự cố diện rộng; Sự cố mạng máy tính; Sự cố một máy tính);
- Và địa điểm xảy ra sự cố.

Bước 4: Phân loại sự cố

Bộ phận ứng cứu xử lý sự cố có trách nhiệm phân loại sự cố:

- Sự cố do lỗi hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc do lỗi đường truyền, hosting,.;
- Sự cố do lỗi của người quản trị, vận hành hệ thống;
- Sự cố do bị tấn công mạng nhưng trên phạm vi 01 máy tính, có thể khắc phục.
- Sự cố về tấn công thay đổi giao diện (deface);
- Sự cố về tấn công lừa đảo (phishing);
- Sự cố về tấn công phát tán mã độc (malware);
- Sự cố về tấn công từ chối dịch vụ (DoS/DDoS);
- Sự cố có yếu tố nước ngoài (hợp tác quốc tế);
- Sự cố tấn công khác.

Bước 5: Báo cáo lãnh đạo, xin ý kiến chỉ đạo

Ngay sau khi phân loại được sự Bộ phận ứng cứu xử lý sự cố có trách nhiệm báo cáo Lãnh đạo đơn vị để xem xét loại sự cố và tuỳ theo đối tượng sẽ tiến hành xử lý.

Trường hợp sự cố được phân loại thông thường thì Bộ phận ứng cứu xử lý sự cố báo cho các bên liên quan để tiếp tục triển khai theo phương án ứng cứu xử lý sự cố an toàn thông tin mạng thông thường theo quy trình tại Phụ lục I (Trích Quy trình ứng cứu xử lý sự cố thông thường của Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017); báo cáo sự cố đến Đội ứng cứu xử lý sự cố an toàn thông tin mạng tỉnh Quảng Ninh (qua Sở Thông tin và Truyền thông) để phối hợp xử lý.

- Trường hợp sự cố được phân loại nghiêm trọng thì gửi báo cáo sự cố đến Đội ứng cứu xử lý sự cố an toàn thông tin mạng tỉnh Quảng Ninh (qua Sở Thông tin và Truyền thông) về sự cố nghiêm trọng để có phương án ứng cứu; và tổ chức ứng cứu, xử lý sự cố: các đơn vị tham gia lực lượng ứng cứu; nguồn lực cần thiết để ứng cứu xử lý sự cố; dự kiến triệu tập bộ phận, cá nhân tác nghiệp ứng cứu khẩn cấp và thực hiện tiếp các bước tiếp theo quy định tại Điều 14 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.

Bước 6: Phối hợp với Đội ứng cứu xử lý sự cố an toàn thông tin mạng tỉnh Quảng Ninh: Thu thập thông tin phục vụ phân tích sự cố; Phân tích sự cố; Xử lý sự cố; Khôi phục, kiểm tra, báo cáo, tổng kết, đánh giá.

CHƯƠNG IV
TỔ CHỨC THỰC HIỆN

Điều 9. Trách nhiệm của bộ phận ứng cứu, xử lý sự cố *(Bộ phận Văn phòng – Thống kê)*

- Chủ trì, phối hợp với cán bộ, công chức người lao động thuộc phường Đại Yên thực hiện các nội dung theo quy định của phương án, quy trình này.

- Làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin (ATTT) mạng trong hệ thống mạng nội bộ của Đại Yên.

- Chủ trì, phối hợp với các phòng, đơn vị tiến hành kiểm tra các công tác bảo đảm ATTT mạng định kỳ hàng năm hoặc theo hướng dẫn của Phòng Văn hóa và Thông tin, Sở Thông tin và Truyền thông.

- Phối hợp Đội ứng cứu xử lý sự cố Tỉnh và thực hiện ứng cứu, xử lý, ngăn chặn, khắc phục sự cố vào các hoạch về bảo đảm ATTT mạng, ứng dụng CNTT.

- Bảo đảm các điều kiện sẵn sàng ứng phó, khắc phục sự cố: đề xuất lãnh đạo phường Đại Yên trang bị, nâng cấp trang thiết bị, công cụ, phương tiện, phương án dự phòng để sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố xảy ra; thuê dịch vụ kỹ thuật và tổ chức, duy trì bộ phận ứng cứu xử lý sự cố.

Điều 10. Trách nhiệm của cán bộ, công chức, người lao động thuộc phường Đại Yên

- Phối hợp với Bộ phận ứng cứu, xử lý sự cố trong quá trình tham gia ứng cứu xử lý sự cố an toàn thông tin khi xảy ra sự cố.

- Tổ chức tuyên truyền, phổ biến các văn bản quy phạm pháp luật nhằm nâng cao nhận thức, kiến thức, kỹ năng về an toàn thông tin mạng.

- Đối với các bộ phận, cá nhân vận hành hệ thống mạng LAN, hệ thống cơ sở dữ liệu, máy chủ: triển khai phương án, quy trình ứng cứu xử lý sự cố cho hệ thống thông tin và các yêu cầu cụ thể của cơ quan; Chủ động trang bị phần mềm chống virus, thiết bị tường lửa cho hệ thống máy tính, hệ thông mạng, hệ thống thông tin; Phối hợp các đơn vị liên quan thực hiện công tác ứng phó khi sự cố ATTT mạng tại cơ quan.

- Thường xuyên kiểm tra việc thực hiện phương án, quy trình ứng cứu xử lý sự cố cho hệ thống thông tin tại cơ quan; chịu trách nhiệm trước Lãnh đạo phường Đại Yên về các vi phạm, thất thoát thông tin, dữ liệu thuộc phạm vi quản lý do không tổ chức, chỉ đạo, kiểm tra cán bộ của đơn vị thực hiện đúng quy định.

- Phối hợp chặt chẽ với Bộ phận ứng cứu, xử lý sự cố trong việc bảo đảm an toàn thông tin, tổ chức xử lý sự cố cho hệ thống thông tin.

- Cán bộ, công chức, người lao động thuộc phường Đại Yên có trách nhiệm: tuân thủ phương án, quy trình ứng cứu xử lý sự cố cho hệ thống thông tin; thông báo kịp thời các vấn đề bất thường liên quan tới an toàn thông tin cho Bộ phận ứng cứu, xử lý sự cố của đơn vị.

- Tham gia 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 do Tỉnh, Sở Thông tin và Truyền thông, Thành phố tổ chức.

Điều 11. Trách nhiệm thi hành

- Cán bộ, công chức người lao động thuộc phường Đại Yên có trách nhiệm phổ biến, quán triệt đến toàn bộ cán bộ, nhân viên trong đơn vị thực hiện các quy định của phương án, quy trình ứng cứu xử lý sự cố cho hệ thống thông tin.

- Trong quá trình thực hiện, nếu có những vấn đề khó khăn, vướng mắc, các bộ phận công tác phản ánh về Bộ phận ứng cứu, xử lý sự cố trình lãnh đạo phường Đại Yên xem xét, sửa đổi, bổ sung phương án cho phù hợp./.