ỦY BAN NHÂN DÂN **THỊ XÃ BỈM SƠN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 4448/QĐ-UBND	*Bỉm Sơn, ngày 08 tháng 12 năm 2017*

QUYẾT ĐỊNH
Về việc ban hành Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước thị xã Bỉm Sơn

ỦY BAN NHÂN DÂN THỊ XÃ BỈM SƠN

Căn cứ Luật Tổ chức Chính quyền địa phương ngày 16/6/2015;

Căn cứ Luật Công nghệ thông tin mạng ngày 29/6/2006;

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

Căn cứ Luật Cơ yếu ngày 26/11/2011;

Căn cứ Luật Ban hành văn bản quy phạm pháp luật ngày 22/6/2015;

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

Căn cứ Nghị định số 34/2016/NĐ-CP ngày 14 tháng 5 năm 2016 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật ban hành văn bản quy phạm pháp luật;

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

Căn cứ Nghị định số 142/2016/NĐ-CP ngày 14 tháng 10 năm 2016 của Chính phủ về ngăn chặn thông tin xung đột trên mạng;

Căn cứ Thông tư số 23/2011/TT-BTTTT ngày 11/8/2011 của Bộ Thông tin & Truyền thông quy định về quản lý, vận hành, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;

Thực hiện Quyết định số 1293/2017/QĐ-UBND ngày 25/4/2017 Ban hành Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan quản lý nhà nước tỉnh Thanh Hóa;

Theo đề nghị của Chánh Văn phòng HĐND&UBND Thị xã,

QUYẾT ĐỊNH:

Điều 1. Ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước thuộc Ủy ban nhân dân thị xã Bỉm Sơn.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày 01/01/2018.

Điều 3. Chánh Văn phòng HĐND&UBND Thị xã, Trưởng các phòng, ban cơ quan UBND Thị xã, UBND các xã phường và Thủ trưởng các cơ quan, đơn vị liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:

- Chủ tịch, các PCT UBND Thị xã (B/c);
- Công an Thị xã (T/h);
- Trưởng các phòng, ban UBND Thị xã (T/h);
- UBND các xã phường (T/h);
- Trung tâm Viễn Thông Bỉm Sơn (T/h);
- Trung tâm Viettel Bỉm Sơn (T/h);
- Lưu: VT.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Bùi Huy Hùng

UỶ BAN NHÂN DÂN **THỊ XÃ BỈM SƠN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**

QUY CHẾ

Đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước thị xã Bỉm Sơn

(Ban hành kèm theo Quyết định số 4448/QĐ-UBND ngày 08 tháng 12 năm 2017 của Ủy ban nhân dân thị xã Bỉm Sơn)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định các nội dung của công tác đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước thuộc thị xã Bỉm Sơn, bao gồm: Bảo vệ thông tin cá nhân, bảo vệ hệ thống thông tin, giám sát an toàn hệ thống thông tin, ngăn chặn xung đột thông tin trên mạng.

Điều 2. Đối tượng áp dụng

1. Quy chế này được áp dụng đối với các cơ quan, đơn vị quản lý Nhà nước trên địa bàn Thị xã, bao phường *(gọi tắt là các cơ quan, đơn vị).*

2. Cán bộ, công chức, viên chức, người lao động *(gọi tắt là cán bộ, công chức)* và các tổ chức, cá nhân có liên quan tham gia vận hành, khai thác các hệ thống thông tin tại cơ quan, đơn vị quy định tại khoản 1 Điều này.

3. Các doanh nghiệp cung cấp dịch vụ viễn thông, công nghệ thông tin (CNTT), Internet; các doanh nghiệp, tổ chức, cá nhân có tham gia vào các hoạt động ứng dụng CNTT của các cơ quan, đơn vị thuộc khoản 1 Điều này.

Điều 3. Giải thích từ ngữ

Trong Quy chế này, các từ ngữ dưới đây được hiểu như sau:

1. Cơ quan nhà nước: Là các cơ quan ban, ngành, đơn vị sự nghiệp thuộc Ủy ban nhân dân Thị xã và Ủy ban nhân dân xã, phường; các tổ chức chính trị, chính trị - xã hội thuộc thị xã Bỉm Sơn.

2. An toàn thông tin: Bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin đối với nguy cơ tự nhiên hoặc do con người gây ra. Việc bảo vệ thông tin, tài sản và con người trong hệ thống thông tin nhằm bảo đảm cho các hệ thống thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy. An toàn thông tin bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng.

3. Hệ thống thông tin: Là một hệ thống bao gồm con người, dữ liệu, các quy trình và công nghệ thông tin tương tác với nhau để thu thập, xử lý, lưu trữ và cung cấp thông tin cần thiết ở đầu ra nhằm hỗ trợ cho một hệ thống.

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

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

6. 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.

7. Mạng nội bộ: Là mạng máy tính trong phạm vi trụ sở của một cơ quan nhà nước.

8. Mạng riêng ảo (VPN - Virtual Private Network): Là một mạng máy tính dành riêng để kết nối các máy tính của các cơ quan nhà nước với nhau thông qua mạng Internet.

9. Thiết bị di động: Các thiết bị di động cá nhân có kết nối vào mạng nội bộ của cơ quan nhà nước như máy tính xách tay, máy tính bảng, điện thoại di động, các thiết bị di động khác.

10. Người dùng: Cán bộ, công chức, viên chức và người lao động của các cơ quan nhà nước sử dụng máy tính, các thiết bị điện tử để xử lý công việc. Các tổ chức, cá nhân có liên quan tham gia, sử dụng các dịch vụ của Trung tâm Dữ liệu thành phố.

Điều 4. Các nguyên tắc về đảm bảo an toàn thông tin mạng

1. Việc đảm bảo an toàn thông tin mạng phải thực hiện theo đúng quy định tại Điều 4 của Luật An toàn thông tin mạng và hướng dẫn của các cơ quan chuyên môn có thẩm quyền.

2. Các văn bản có nội dung "Mật" trở lên khi gửi, nhận qua mạng phải được thủ trưởng cơ quan, đơn vị cho phép và phải được mã hóa theo quy định của Luật cơ yếu và các văn bản pháp luật liên quan.

3. Việc đảm bảo an toàn thông tin mạng không được làm ảnh hưởng đến các hoạt động bình thường của các cơ quan quản lý nhà nước.

4. Công tác đảm bảo an toàn thông tin mạng phải được thực hiện trên cơ sở có sự phối hợp chặt chẽ giữa các cơ quan, đơn vị và cá nhân.

Chương II
NỘI DUNG ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 5. Đảm bảo an toàn máy chủ, máy trạm, các thiết bị di động và cơ chế sao lưu, phục hồi.

Kiểm soát chặt chẽ việc cài đặt các phần mềm mới lên máy chủ, máy trạm và các thiết bị di động. Các phần mềm được cài đặt trên máy chủ, máy trạm và các thiết bị di động (bao gồm hệ điều hành, các phần mềm ứng dụng CNTT) 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 ít nhất hàng tuần.

Quy định cơ chế sao lưu định kỳ ít nhất 01 tháng/01 lần các tập tin ghi lại sự kiện xảy ra trong hệ điều hành hoặc các phần mềm trong quá trình hoạt động, cơ sở dữ liệu và các dữ liệu quan trọng được triển khai, lưu trữ (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 (như: Đĩa quang, ổ cứng 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.

Điều 6. Bảo vệ hệ thống thông tin mạng.

1. Đối với các cơ quan, đơn vị:

Thực hiện việc phân loại thông tin, phân loại cấp độ an toàn cho hệ thống thông tin thuộc quyền quản lý theo thuộc tính bí mật để có biện pháp bảo vệ phù hợp, cụ thể:

a) Việc phân loại thông tin được thực hiện theo các quy định tại Điều 9 Luật An toàn thông tin mạng và khoản 1, Điều 6 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ.

b) Việc quản lý gửi thông tin trên mạng phải tuân thủ theo các nội dung quy định tại Điều 10 Luật An toàn thông tin mạng và các quy định sau:

- Việc trao đổi văn bản, tài liệu điện tử của cơ quan (kể cả tài liệu tham khảo) chỉ thực hiện trên hệ thống phần mềm quản lý văn bản và hồ sơ công việc đã được triển khai hoặc sử dụng hệ thống thư điện tử công vụ của huyện hoặc trên các phần mềm ứng dụng của nội bộ ngành chuyển giao ứng dụng.

- Khi phát hành và gửi qua mạng các văn bản của các cơ quan quản lý nhà nước phải được thực hiện ký số trước khi gửi.

c) Việc phân loại cấp độ an toàn cho hệ thống thông tin được thực hiện theo các quy định tại Điều 21 Luật An toàn thông tin mạng; khoản 2 Điều 6; các Điều 7, 8, 9, 10, 11 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ.

d) Nội dung bảo vệ hệ thống thông tin được thực hiện theo các quy định tại các Điều 22, 23 Luật An toàn thông tin mạng và trong Chương IV Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ. Khi xây dựng, nâng cấp, mở rộng hạ tầng kỹ thuật CNTT, các hệ thống thông tin của cơ quan, đơn vị phải có phương án đảm bảo an toàn thông tin mạng và phải được Sở Thông tin và Truyền thông thẩm định trước khi trình cấp có thẩm quyền phê duyệt và tuân thủ các quy định sau:

- Hệ thống mạng nội bộ (mạng LAN) của các cơ quan, đơn vị được tổ chức theo hướng sử dụng máy chủ để quản lý các máy trạm trong hệ thống mạng, không sử dụng mô hình mạng ngang hàng (không có máy chủ quản lý). Các máy chủ, máy trạm, hệ thống lưu trữ nội bộ, thiết bị mạng, mạng không dây (wifi) phải được bảo vệ bởi mật khẩu an toàn. 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 ít nhất 03 tháng/01 lần. Tất cả các máy tính tại các cơ quan, đơn vị phải được cài đặt các phần mềm bảo vệ, phòng chống virus, cập nhập bản vá lỗi thường xuyên.

- Các thiết bị CNTT dùng để soạn thảo, in ấn văn bản, lưu trữ thông tin bí mật nhà nước trong các cơ quan, đơn vị phải được bố trí riêng, tiến hành ở nơi đảm bảo bí mật, an toàn; không được kết nối vào mạng LAN của đơn vị. Đặc biệt là không được sử dụng máy tính đã nối mạng Internet đánh máy, in, sao tài liệu mật. Trên máy tính này phải thực hiện các chế độ mã hóa, phân quyền và đặt mật khẩu (password) cho người được giao sử dụng để đảm bảo an toàn, bảo mật thông tin.

- Khi thực hiện di chuyển các trang thiết bị CNTT lưu trữ dữ liệu, thông tin thuộc danh mục bí mật Nhà nước phải được tổ chức quản lý, giám sát chặt chẽ theo quy định của pháp luật về bảo vệ bí mật nhà nước.

- Các cơ quan, đơn vị, cá nhân tham gia sử dụng mạng chuyên dùng thực hiện nghiêm túc các nội dung về đảm bảo an toàn thông tin mạng trên mạng truyền số liệu chuyên dùng được quy định tại các Điều 10, 11, 12 của Thông tư số 23/2011/TT-BTTTT ngày 11/8/2011 của Bộ Thông tin và truyền thông.

2. Đối với các đơn vị, doanh nghiệp cung cấp các dịch vụ viễn thông, CNTT, Internet cho cơ quan quản lý nhà nước thị xã Bỉm Sơn:

Thực hiện các nội dung liên quan đến hoạt động bảo đảm an toàn thông tin mạng theo Điều 22 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ; Điều 7, Điều 9, Thông tư số 23/2011/TT-BTTTT ngày 11/8/2011 của Bộ Thông tin và Truyền thông và các quy định sau:

a) Thực hiện các quy định của pháp luật về lưu trữ thông tin, bảo vệ thông tin cá nhân, thông tin riêng của các cơ quan, đơn vị. Áp dụng và tổ chức thực hiện các biện pháp ngăn chặn việc gửi thông tin vi phạm quy định của pháp luật khi nhận được thông báo của cơ quan, đơn vị. Cung cấp các điều kiện kỹ thuật và nghiệp vụ cần thiết để thực hiện nhiệm vụ, bảo đảm an toàn thông tin mạng theo yêu cầu của cơ quan nhà nước có thẩm quyền.

b) Phải có hệ thống lọc phần mềm độc hại trong quá trình thực hiện các dịch vụ gửi, nhận, lưu trữ thông tin trên hệ thống của mình; có biện pháp quản lý, phòng ngừa, phát hiện, ngăn chặn phát tán phần mềm độc hại xử lý theo yêu cầu của cơ quan nhà nước có thẩm quyền; quản lý, phối hợp ngăn chặn mất an toàn thông tin mạng xuất phát từ tài nguyên Internet, từ khách hàng của mình; phối hợp, kết nối định tuyến để đảm bảo hệ thống máy chủ có tên miền quốc gia Việt Nam hoạt động an toàn, ổn định.

3. Đối với các cơ quan nhà nước có sử dụng đường truyền Internet ngoài đường truyền số liệu chuyên dùng trong hệ thống các cơ quan Đảng, Nhà nước, phải thông báo về Sở Thông tin và Truyền thông để được hướng dẫn đấu nối, thiết lập các thông số của các thiết bị định tuyến, cấu hình địa chỉ IP cho hệ thống

mạng nội bộ, các máy chủ, máy trạm trong cơ quan thống nhất với toàn hệ thống.

Điều 7. Bảo vệ thông tin cá nhân.

1. Cán bộ, công chức trong các cơ quan quản lý nhà nước có trách nhiệm tự bảo vệ thông tin cá nhân của mình và tuân thủ các quy định tại khoản 1, khoản 2 Điều 10; khoản 1, khoản 4 Điều 16; khoản 3 Điều 17; khoản 1 Điều 18 Luật An toàn thông tin mạng và trong các văn bản pháp luật có liên quan.

2. Cán bộ, công chức trong các cơ quan quản lý nhà nước khi sử dụng, khai thác các hệ thống thông tin của cơ quan, đơn vị và các phần mềm ứng dụng dùng chung của Thị xã phải có trách nhiệm:

a) Tự quản lý và tự chịu trách nhiệm về bảo vệ thông tin cá nhân đã được khai báo trong các hệ thống thông tin; không tiết lộ tài khoản đăng nhập, đấu nối, truy cập trái phép vào các phần mềm dùng chung của Thị xã.

b) Ngay sau khi được cấp tài khoản truy cập vào các phần mềm dùng chung của Thị xã, cơ quan, đơn vị, cá nhân được cấp tài khoản phải thực hiện việc đổi mật khẩu.

c) Khi khai thác, sử dụng các phần mềm dùng chung của huyện tại các điểm truy cập Internet công cộng, tuyệt đối không đặt chế độ lưu trữ mật khẩu trong quá trình sử dụng.

3. Các cơ quan, đơn vị, cá nhân khi xử lý thông tin cá nhân phải tuân thủ đầy đủ các nội dung theo quy định tại khoản 2, 3, 4, 5 Điều 16; khoản 1, 2 Điều 17; khoản 3 Điều 18; Điều 19 của Luật An toàn thông tin và các quy định sau:

a) Quản lý và phân quyền truy cập trong các phần mềm ứng dụng, hệ thống thông tin, cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ, quyền hạn của người tham gia quản lý, vận hành, khai thác, sử dụng các phần mêm ứng dụng, hệ thống thông tin, cơ sở dữ liệu.

b) Khi cán bộ, công chức, viên chức đã nghỉ việc hoặc chuyển công tác, các cơ quan, đơn vị phải thực hiện việc thu hồi các thiết bị CNTT liên quan; đồng thời phải đề xuất với cơ quan quản lý, quản trị phần mềm ứng dụng, hệ thống thông tin, cơ sở dữ liệu để thực hiện các biện pháp kỹ thuật cập nhật lại, khóa hoặc hủy tài khoản người dùng.

Điều 8. Đảm bảo an toàn thông tin, dữ liệu

1. 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.

2. Trong trao đổi thông tin, dữ liệu phục vụ công việc, cơ quan nhà nước, cán bộ công chức viên chức phải sử dụng hệ thống thông tin do cơ quan nhà nước có thẩm quyền triển khai như: Phần mềm Quản lý văn bản & Hồ sơ công việc, phần mềm Theo dõi nhiệm vụ, phần mềm Một cửa điện tử, Thư điện tử công vụ. Không sử dụng các phương tiện trao đổi thông tin dữ liệu, hệ thống thư điện tử, lưu trữ điện tử công cộng, mạng xã hội trên Internet trong hoạt động của

cơ quan nhà nước.

Điều 9. Giám sát an toàn hệ thống thông tin mạng

1. Đối với các cơ quan, đơn vị.

Tổ chức thực hiện việc giám sát an toàn hệ thống thông tin của cơ quan, đơn vị trực tiếp quản lý. Nội dung và đối tượng giám sát thực hiện theo quy định tại các khoản 1, 2 Điều 24 của Luật An toàn thông tin mạng; đồng thời, thực hiện việc lưu trữ nhật ký tình trạng hoạt động của các hệ thống thông tin tại các máy chủ trong thời gian ít nhất là 30 ngày để phục vụ các công tác đảm bảo an toàn thông tin mạng.

2. Đối với các doanh nghiệp cung cấp các dịch vụ viễn thông, CNTT, Internet có trách nhiệm thực hiện theo quy định tại khoản 3 Điều 24 của Luật An toàn thông tin mạng.

Điều 10. Ngăn chặn xung đột thông tin trên mạng.

1. Đối với các cơ quan, đơn vị là chủ quản trực tiếp các hệ thống thông tin:

a) Các cơ quan, đơn vị trong phạm vi quyền hạn của mình có trách nhiệm ngăn chặn xung đột thông tin trên mạng theo các nội dung quy định tại khoản 1 Điều 28 Luật An toàn thông tin mạng; khoản 1 Điều 8; khoản 1, Điều 9; các khoản 3, 4, 5, Điều 12; các khoản 1, 2, Điều 14 và Điều 27 Nghị định số 142/2016/NĐ-CP ngày 14/10/2016 của Chính phủ và các quy định sau:

- Phải thực hiện các biện pháp bảo vệ hệ thống thông tin của mình quản lý, không để các phần tử xấu lợi dụng hệ thống thông tin để thâm nhập, truy cập trái phép vào các Trung tâm đang quản lý các hệ thống thông tin, cơ sở dữ liệu của huyện.

- Quản lý chặt chẽ các tài khoản đã cung cấp cho người dùng trong cơ quan, đơn vị.

b) Cán bộ, công chức của các cơ quan, đơn vị có trách nhiệm ngăn chặn xung đột thông tin trên mạng theo các nội dung quy định tại khoản 1 Điều 28 Luật An toàn thông tin mạng; khoản 1 Điều 7; các khoản 4, 5 Điều 12 và Điều 27 Nghị định số 142/2016/NĐ-CP ngày 14/10/2016 của Chính phủ.

2. Văn phòng HĐND&UBND Thị xã.

Chủ trì, phối hợp với các đơn vị liên quan của sở Thông tin và Truyền thông và các cơ quan nghiệp vụ, các ngành, đơn vị liên quan để tham mưu và tổ chức thực hiện các giải pháp ngăn chặn xung đột thông tin trên mạng theo các nội dung được quy định tại các khoản 2, 3 Điều 6; các khoản 2, 3 Điều 9; khoản 3 Điều 14; các khoản 1, 3 Điều 15 và các Điều 16, 17, 18 của Nghị định số 142/2016/NĐ-CP ngày 14/10/2016 của Chính phủ và các quy định sau:

a) Chủ trì, phối hợp với các đơn vị liên quan thực hiện ngăn chặn xung đột thông tin trên mạng bao gồm giám sát, phát hiện, cảnh báo, xác định nguồn gốc và khắc phục xung đột thông tin trên mạng.

b) Phối hợp với phòng Văn hóa - Thông tin chỉ đạo các cơ quan nghiệp vụ tổ chức triển khai các phương án bảo vệ các hệ thống thông tin trong phạm vi

quản lý; sẵn sàng huy động lực lượng, phương tiện tham gia hoạt động ngăn chặn xung đột thông tin trên mạng, thuộc phạm vi quản lý theo quy định của pháp luật.

3. Các doanh nghiệp cung cấp dịch vụ viễn thông, CNTT, Internet cho các cơ quan quản lý nhà nước, trong phạm vi quyền hạn của mình có trách nhiệm ngăn chặn xung đột thông tin trên mạng theo các nội dung quy định tại khoản 1, Điều 28; khoản 1, Điều 29 Luật An toàn thông tin mạng và các quy định tại khoản 5 Điều 12; Điều 28 Nghị định số 142/2016/NĐ-CP ngày 14/10/2016 của Chính phủ.

Điều 10. Quy trình phối hợp ứng cứu sự cố về an toàn thông tin

Cơ quan nhà nước khi phát hiện hệ thống có nguy cơ mất an toàn như: Hệ thống hoạt động chậm bất thường, không truy cập được hệ thống, nội dung thông tin bị thay đổi không chủ động hoặc các dấu hiệu bất thường khácthì tiến hành quy trình ứng cứu sự cố theo các bước sau:

1. Bước 1: Nếu hệ thống có nguy cơ mất an toàn thông tin thuộc thẩm quyền cơ quan nhà nước trực tiếp quản lý thì thực hiện tiếp Bước 2. Nếu hệ thống có nguy cơ mất an toàn thông tin thuộc Sở Thông tin và Truyền thông quản lý (các hệ thống được triển khai tập trung tại Trung tâm Dữ liệu Tỉnh) thì thực hiện tiếp Bước 3;

2. Bước 2: Tiến hành xử lý sự cố theo quy chế nội bộ của cơ quan nhà nước. Nếu sự cố được khắc phục thì lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố. Khi sự cố vượt quá khả năng xử lý của cơ quan, lập biên bản ghi nhận và thực hiện tiếp Bước 3;

3. Bước 3: Báo cáo sự cố đến Sở Thông tin và Truyền thông để thực hiện theo hướng dẫn và thực hiện tiếp Bước 4;

4. Bước 4: Phối hợp với Sở Thông tin và Truyền thông và các cơ quan,tổ chức có liên quan để tiến hành khắc phục sự cố và thực hiện tiếp Bước 5;

5. Bước 5: Lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 11. Trách nhiệm của các cơ quan nhà nước

1. Thủ trưởng các cơ quan nhà nước tổ chức thực hiện nghiêm túc các quy định tại Quy chế này và chịu trách nhiệm trước Ủy ban nhân dân Thị xã trong công tác đảm bảo an toàn thông tin của đơn vị mình.

2. Ban hành quy chế, quy trình nội bộ về đảm bảo an toàn thông tin phù hợp với Quy chế này và các quy định của pháp luật.

3. Đưa nội dung thực hiện đảm bảo an toàn thông tin vào kế hoạch ứng dụng công nghệ thông tin hàng năm của đơn vị.

4. Tuyên truyền, phổ biến Quy chế này và các quy định khác của pháp

luật có liên quan về an toàn thông tin trong phạm vi trách nhiệm và quyền hạn.

5. Phân công một bộ phận hoặc cán bộ phụ trách đảm bảo an toàn thông tin của đơn vị; tạo điều kiện để các cán bộ phụ trách an toàn thông tin được học tập, nâng cao trình độ về an toàn thông tin, đồng thời tạo điều kiện để cán bộ, công chức, viên chức và người lao động tham gia tập huấn kiến thức về an toàn thông tin.

6. Thực hiện tốt việc phối hợp ứng cứu sự cố an toàn khi có nguy cơ mất an toàn thông tin, tạo điều kiện thuận lợi cho các cơ quan chức năng, tổ chức tham gia khắc phục sự cố và thực hiện đúng theo hướng dẫn.

7. Phối hợp với đoàn kiểm tra trong công tác thanh tra, kiểm tra việc thực hiện đảm bảo an toàn thông tin.

8. Nghiêm túc thực hiện các biện pháp quản lý, các yêu cầu cam kết về đảm bảo an toàn thông tin đối với các tổ chức, cá nhân khi tham gia vào các hệ thống thông tin do đơn vị mình quản lý.

9. Báo cáo tình hình, kết quả thực hiện công tác đảm bảo an toàn thông tin tại cơ quan nhà nước theo định kỳ hoặc đột xuất khi được yêu cầu.

10. Bố trí kinh phí cho việc mua sắm, nâng cấp trang thiết bị CNTT để tăng cường năng lực đảm bảo an toàn thông tin mạng của các cơ quan, đơn vị theo quy định của Nhà nước.

Điều 12. Trách nhiệm của Văn phòng HĐND&UBND Thị xã.

1. Chủ trì phối hợp với Phòng Quản lý Cổng TTĐT & CNTT – UBND Tỉnh và Sở Thông tin & Truyền thông Thanh Hóa xử lý kịp thời sự cố mất an toàn thông tin mạng tại cơ quan nếu xảy ra.

2. Hàng năm, tham mưu xây dựng kế hoạch ứng dụng và phát triển công nghệ thông tin trong cơ quan nhà nước thị xã Bỉm Sơn, trong đó lồng ghép nội dung đảm bảo an toàn thông tin các hệ thống thông tin được Ủy ban nhân dân Thị xã giao quản lý.

3. Thực hiện nhiệm vụ cảnh báo về nguy cơ hoặc sự cố mất an toàn thông tin mạng; tiếp nhận thông tin, hỗ trợ kỹ thuật và tham gia xử lý các sự cố về an toàn thông tin mạng cho các cơ quan, đơn vị. Tổ chức thực hiện các hoạt động điều phối, ứng cứu sự cố máy tính trong cơ quan UBND Thị xã.

4. Phối hợp với phòng Văn Hóa – Thông tin tổ chức kiểm tra, giám sát việc thực hiện đảm bảo an toàn thông tin mạng tại các cơ quan, đơn vị, tại các doanh nghiệp cung cấp dịch vụ viễn thông, CNTT, Internet trên địa bàn Thị xã để kịp thời phát hiện, xử lý các hành vi vi phạm an toàn thông tin mạng.

5. Tổng hợp, báo cáo Ủy ban nhân dân Thị xã theo định kỳ 06 tháng hoặc đột xuất về công tác đảm bảo an toàn thông tin của Thị xã và các vấn đề về an toàn thông tin quan trọng phát sinh.

Điều 13. Trách nhiệm của phòng Văn hóa và Thông tin.

1. Tham mưu cho UBND Thị xã, Chủ tịch UBND Thị xã ban hành các văn bản chỉ đạo, các chương trình, kế hoạch để tổ chức thực hiện tốt nhiệm vụ đảm

bảo an toàn thông tin mạng trong các cơ quan, đơn vị trên địa bàn Thị xã. Chịu trách nhiệm trước UBND Thị xã về công tác đảm bảo an toàn thông tin mạng trong hoạt động của các cơ quan, đơn vị trên địa bàn.

2. Thực hiện vai trò, nhiệm vụ của cơ quan chuyên trách, giúp UBND huyện thực hiện quản lý nhà nước về đảm bảo an toàn thông tin mạng trên địa bàn huyện:

a) Ban hành đầy đủ và kịp thời các văn bản hướng dẫn cho các cơ quan, đơn vị về đảm bảo an toàn thông tin mạng theo các nội dung chỉ đạo của UBND Tỉnh và Sở Thông tin và Truyền thông Thanh Hóa.

b) Chủ trì, phối hợp với các cơ quan, đơn vị liên quan lồng ghép các đợt kiểm tra văn hóa, thông tin tổ chức kiểm tra, giám sát việc thực hiện đảm bảo an toàn thông tin mạng tại các cơ quan, đơn vị, tại các doanh nghiệp cung cấp dịch vụ viễn thông, CNTT, Internet trên địa bàn huyện để kịp thời phát hiện, xử lý các hành vi vi phạm an toàn thông tin mạng.

Điều 14. Trách nhiệm của Công an Thị xã.

1. Chủ động triển khai các biện pháp, công tác nghiệp vụ phòng ngừa, phát hiện, đấu tranh ngăn chặn hoạt động xâm hại đến an toàn thông tin mạng trong các cơ quan, đơn vị.

2. Phối hợp với phòng Văn hóa và Thông tin và các cơ quan, đơn vị có liên quan thanh tra, kiểm tra, xử lý vi phạm về an toàn thông tin mạng trên địa bàn huyện.

Điều 15. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các cơ quan nhà nước

1. Trách nhiệm của cán bộ phụ trách an toàn thông tin tại các cơ quan nhà nước:

a) Tham mưu lãnh đạo ban hành các quy định, biện pháp nhằm đảm bảo an toàn thông tin, tham mưu chuyên môn và vận hành an toàn hệ thống thông tin của đơn vị theo nhiệm vụ được Thủ trưởng đơn vị phân công và theo các nội dung của Quy chế này.

b) Thực hiện giám sát, theo dõi việc tuân thủ thực hiện quy định về an toàn thông tin, kịp thời phát hiện các nguy cơ mất an toàn thông tin để báo cáo, tham mưu lãnh đạo chỉ đạo thực hiện.

c) Phối hợp với các cơ quan, tổ chức, cá nhân liên quan trong việc kiểm tra, khắc phục sự cố mất an toàn thông tin.

d) Tham gia các chương trình đào tạo, tập huấn chuyên môn, hội nghị về an toàn thông tin nhằm nâng cao nhận thức, năng lực chuyên môn, nghiệp vụ.

2. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các cơ quan nhà nước:

a) Thực hiện nghiêm các quy chế nội bộ, quy trình về an toàn thông tin cũng như các quy định khác của pháp luật, nâng cao ý thức cảnh giác, trách nhiệm đảm bảo an toàn thông tin tại đơn vị.

b) Khi phát hiện sự cố phải báo cáo ngay với cấp trên và bộ phận hoặc cán bộ phụ trách an toàn thông tin để kịp thời ngăn chặn, xử lý.

c) Tham gia các chương trình đào tạo, tập huấn, hội nghị về an toàn thông tin nhằm nâng cao nhận thức và nắm thông tin (Nếu có).

d) Nghiêm cấm mọi hành vi cố ý lan truyền, phát tán virus lên mạng, phát tán thư rác, sử dụng các phần mềm bất hợp pháp để truy xuất, phá hoại hệ thống; cấm truyền bá văn hóa phẩm đồi trụy, nội dung không phù hợp với văn hóa Việt Nam, nội dung có ý xuyên tạc, chống đối nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam.

đ) Không được đánh cắp và sử dụng trái phép mật mã, thông tin riêng của các đơn vị, người dùng hoặc phổ biến cho người khác sử dụng trên hệ thống mạng LAN.

e) Nghiêm cấm mọi hành vi khác theo Điều 5 của Nghị định số 72/2013/NĐ-CP ngày 15 tháng 7 năm 2013 của Chính phủ về việc quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng.

Điều 16. Trách nhiệm của các doanh nghiệp cung cấp dịch vụ viễn thông, CNTT và Internet cho các cơ quan quản lý nhà nước thị xã Bỉm Sơn.

1. Đầu tư xây dựng, trang bị hạ tầng kỹ thuật đáp ứng đầy đủ các yêu cầu, tiêu chuẩn kỹ thuật theo quy định của Bộ Thông tin và Truyền thông về an ninh mạng và an toàn thông tin và các nội dung quy định tại Quy chế này.

2. Phối hợp với phòng Văn hóa và Thông tin để tham gia các hoạt động điều phối, ứng cứu, khắc phục sự cố thông tin đảm bảo an toàn thông tin mạng cho các cơ quan, đơn vị trong quá trình sử dụng, khai thác dịch vụ.

Điều 17. Điều khoản thi hành

Trong quá trình thực hiện, nếu có vướng mắc, phát sinh; các cơ quan, đơn vị kịp thời phản ánh về Văn phòng HĐND&UBND Thị xã để tổng hợp, báo cáo Chủ tịch UBND Thị xã xem xét sửa đổi, bổ sung cho phù hợp./.