ỦY BAN NHÂN DÂN THỊ XÃ BUÔN HỒ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 1444 /QĐ-UBND	*Buôn Hồ, ngày 18 tháng 5 năm 2023*

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của các cơ quan nhà nước trên địa bàn thị xã Buôn Hồ

ỦY BAN NHÂN DÂN THỊ XÃ BUÔN HỒ

Căn cứ Luật Tổ chức Chính quyền địa phương ngày 19 tháng 6 năm 2015;

Căn cứ Luật Giao dịch Điện tử ngày 29 tháng 11 năm 2005;

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 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 142/2016/NĐ-CP ngày 14 tháng 10 năm 2016 của Chính phủ về Ngăn chặn xung đột thông tin trên mạng;

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 Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông về 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 Thông tư số 27/2017/TT-BTTTT ngày 20 tháng 10 năm 2017 của Bộ Thông tin và Truyền thông quy định về việc 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;

Theo đề nghị của phòng Văn hóa - Thông tin thị xã tại Tờ trình số 114/TTr-VHTT ngày 26/4/2023 về việc ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của các cơ quan nhà nước trên địa bàn thị xã Buôn Hồ.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của các cơ quan nhà nước trên địa bàn thị xã Buôn Hồ.

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

Điều 3. Chánh Văn phòng HĐND-UBND thị xã; Trưởng các phòng, ban, đơn vị thị xã; Chủ tịch UBND các xã, phường; Thủ trưởng các cơ quan, đơn vị và cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

***Nơi nhận*:**
- Như Điều 3;
- Sở TTTT tỉnh;
- TT Thị ủy;
- TT HĐND thị xã;

(b/c)

- CT, các PCT UBND thị xã;
- Các Ban HĐND thị xã;
- UBMTTQVN thị xã và các tổ chức đoàn thể thị xã;
- Lưu: VT, VHTT(CH- b).

TM. ỦY BAN NHÂN DÂN
KT.CHỦ TỊCH
PHÓ CHỦ TỊCH

Võ Văn Dũng

ỦY BAN NHÂN DÂN THỊ XÃ BUÔN HỒ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc

QUY CHẾ
Bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng Công nghệ thông tin, chuyển đổi số của các cơ quan nhà nước trên địa bàn thị xã Buôn Hồ

(Ban hành kèm theo Quyết định số 1444/QĐ-UBND ngày 18 tháng 5 năm 2023 của Ủy ban nhân dân thị xã Buôn Hồ)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh:

Quy chế này quy định biện pháp, chính sách quản lý nhằm bảo đảm an toàn thông tin các hệ thống thông tin trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của cơ quan nhà nước gồm các phòng, ban, đơn vị thuộc Ủy ban nhân dân thị xã Buôn Hồ và Ủy ban nhân dân các xã, phường trên địa bàn thị xã Buôn Hồ (gọi chung là cơ quan, đơn vị).

2. Đối tượng áp dụng:

a) 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.

b) 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, chuyển đổi số của các cơ quan, đơn vị thuộc khoản 1 Điều này.

c) Khuyến khích các cơ quan, đơn vị khác hoạt động ứng dụng và phát triển CNTT trên địa bàn thị xã Buôn Hồ áp dụng quy chế này.

Điều 2. Giải thích từ ngữ

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

1. *An toàn thông tin* là 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.

2. *Hệ thống thông tin* là tập hợp thiết bị phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin.

3. *Xâm phạm an toàn thông tin* là hành vi truy cập, sử dụng, tiết lộ, làm gián đoạn, sửa đổi, làm sai lệch chức năng, phá hoại trái phép thông tin và hệ thống thông tin.

4. *Nguy cơ mất an toàn thông tin* là những nhân tố bên trong hoặc bên ngoài có khả năng làm ảnh hưởng tới trạng thái an toàn thông tin.

5. *Mạng* là khái niệm chung dùng để chỉ mạng viễn thông cố định, di động, internet và mạng máy tính.

Điều 3. Nguyên tắc bảo đảm an toàn thông tin

1. Cơ quan, tổ chức, cá nhân có trách nhiệm bảo đảm an toàn thông tin mạng. Hoạt động an toàn thông tin mạng của cơ quan, tổ chức, cá nhân phải đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước, giữ vững ổn định chính trị, trật tự, an toàn xã hội và thúc đẩy phát triển kinh tế - xã hội.

2. Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác.

3. Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức.

4. Hoạt động an toàn thông tin mạng phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.

5. Tuân thủ các nguyên tắc, các tiêu chuẩn, quy chuẩn kỹ thuật về bảo mật, an toàn thông tin; chấp hành hướng dẫn của cơ quan chuyên môn quản lý nhà nước về thông tin và truyền thông về các giải pháp, biện pháp, kỹ thuật về quản lý, bảo mật, an toàn thông tin.

6. Kết hợp nhiều biện pháp bảo đảm an toàn thông tin, nhằm phát hiện và ngăn chặn kịp thời các nguy cơ mất an toàn thông tin.

7. 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
BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 4. Quản lý an toàn thông tin của các cơ quan, đơn vị đối với người sử dụng

1. Cơ quan, đơn vị có trách nhiệm phổ biến các quy định về bảo đảm an toàn thông tin mạng cho toàn thể cán bộ, công chức tại cơ quan, đơn vị.

2. Quản lý và phân quyền truy cập trong các phần mềm, nền tảng 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.

3. Khi cán bộ, công chức đã nghỉ việc hoặc chuyển công tác, cơ quan, đơn vị phải thực hiện thu hồi các thiết bị công nghệ thông tin thuộc quyền quản lý; đồng thời thông báo bằng văn bản đến cơ quan quản lý, quản trị phần mềm, nền tảng ứng dụng dùng chung, hệ thống thông tin, cơ sở dữ liệu để thực hiện các biện pháp kỹ thuật cập nhật lại thông tin tài khoản, khóa hoặc hủy tài khoản người dùng.

Điều 5. Quản lý truy cập

1. Đối với người sử dụng

a) Có trách nhiệm bảo vệ bí mật thông tin tài khoản cá nhân, tài khoản của cơ quan, đơn vị khi được phân công sử dụng để truy cập các hệ thống phần mềm dùng chung, nền tảng ứng dụng, hệ thống thông tin, cơ sở dữ liệu của cơ quan, đơn vị.

b) Không đặt chế độ lưu trữ mật khẩu trên các ứng dụng, công cụ truy cập để tự động điền thông tin đăng nhập vào các hệ thống phần mềm dùng chung, nền tảng ứng dụng, hệ thống thông tin, cơ sở dữ liệu của cơ quan, đơn vị.

c) Thiết lập mật khẩu đăng nhập vào các hệ thống phần mềm dùng chung, nền tảng ứng dụng, hệ thống thông tin, cơ sở dữ liệu của cơ quan, đơn vị phải đảm bảo có độ phức tạp cao, độ dài tối thiểu 8 ký tự, có ký tự chữ hoa, ký tự chữ thường, ký tự số và ký tự đặc biệt. Mật khẩu phải được thay đổi ít nhất 03 tháng/lần.

2. Đối với người quản trị

a) Người được giao tài khoản quản trị các hệ thống phần mềm dùng chung, nền tảng ứng dụng, hệ thống thông tin, cơ sở dữ liệu của cơ quan, đơn vị phải thực hiện cập nhật thông tin tài khoản người dùng vào hệ thống ngay khi nhận được văn bản thông báo thay đổi người dùng.

b) Bàn giao thông tin tài khoản quản trị các hệ thống phần mềm dùng chung, nền tảng ứng dụng, hệ thống thông tin, cơ sở dữ liệu của cơ quan, đơn vị cho lãnh đạo quản lý trực tiếp.

Điều 6. Bảo vệ thông tin cá nhân

1. Cán bộ, công chức 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.

Khi sử dụng, khai thác các hệ thống thông tin của cơ quan, đơn vị và các phần mềm ứng dụng dùng chung của tỉnh, có trách nhiệm:

a) Tự quản lý và 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 tỉnh, cơ quan, đơn vị.

b) Phải thực hiện việc đổi mật khẩu ngay sau khi được cấp tài khoản truy cập vào các phần mềm dùng chung của tỉnh, cơ quan, đơn vị.

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

2. 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 mạng 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 mềm 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 thông báo ngay bằng văn bản đến 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 7. Quy định bảo vệ hệ thống thông tin mạng

Các cơ quan nhà nước trên địa bàn thị xã thực hiện:

a) Trang bị đầy đủ các kiến thức bảo mật cơ bản cho cán bộ, công chức trước khi cho phép truy nhập và sử dụng hệ thống thông tin.

b) Phân công cán bộ, công chức chuyên trách hoặc phụ trách CNTT, để quản lý kỹ thuật nghiệp vụ về an toàn thông tin tại đơn vị.

c) Thủ trưởng cơ quan, đơn vị tạo điều kiện để cán bộ, công chức chuyên trách hoặc phụ trách CNTT học tập, tiếp thu công nghệ, kiến thức an toàn thông tin.

d) Hàng năm, xác định các nhiệm vụ bảo đảm an toàn thông tin hệ thống (mở rộng, nâng cấp trang thiết bị; đào tạo, bồi dưỡng kiến thức CNTT, ...) để đề xuất kinh phí đến cơ quan có thẩm quyền hoặc phân bổ kinh phí duy trì hoạt động hệ thống thông tin hiệu quả.

đ) 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 cấp có thẩm quyền phê duyệt.

e) Quản lý các tài khoản của hệ thống thông tin, tài khoản người dùng bao gồm: Tạo mới, sửa đổi, hủy các tài khoản. Thường xuyên kiểm tra các tài khoản

của hệ thống thông tin; triển khai các công cụ để hỗ trợ việc quản lý các tài khoản của hệ thống thông tin.

Điều 8. Bảo vệ bí mật nhà nước trong hoạt động ứng dụng công nghệ thông tin

1. Quy định về soạn thảo, in ấn, phát hành và sao chụp tài liệu mật

a) Không được sử dụng máy tính kết nối mạng Internet để soạn thảo văn bản mật; chuyển giao, lưu trữ thông tin có nội dung thuộc bí mật nhà nước; Không cung cấp tin, tài liệu và đưa thông tin bí mật nhà nước lên không gian mạng.

b) Không được in, sao chụp tài liệu bí mật nhà nước trên các thiết bị kết nối mạng internet.

c) Phải bố trí 01 máy tính riêng, không kết nối mạng nội bộ và mạng Internet dùng để quản lý, soạn thảo các tài liệu mật của nhà nước theo quy định.

2. Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật, các cơ quan, đơn vị phải báo cáo cho người có thẩm quyền. Không được cho phép các tổ chức, cá nhân không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố.

3. Trước khi thanh lý các máy tính trong các cơ quan nhà nước, cán bộ chuyên trách công nghệ thông tin phải dùng các biện pháp kỹ thuật xoá bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 9. Trách nhiệm của Phòng Văn hóa - Thông tin thị xã

1. Tham mưu Ủy ban nhân dân thị xã về công tác bảo đảm an toàn thông tin trên địa bàn thị xã và chịu trách nhiệm trước Ủy ban nhân dân thị xã trong việc bảo đảm an toàn thông tin.

2. Chủ trì, phối hợp với các cơ quan, đơn vị có liên quan tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hàng năm hoặc theo chỉ đạo của Ủy ban nhân dân thị xã đối với các cơ quan nhà nước đóng trên địa bàn thị xã.

3. Hàng năm, cử cán bộ tham gia các lớp đào tạo, tập huấn về công tác bảo đảm an toàn thông tin mạng cho cán bộ phụ trách an toàn thông tin mạng. Tổ chức tuyên truyền về an toàn thông tin mạng trong công tác quản lý nhà nước trên địa bàn thị xã.

4. Phối hợp với Công an thị xã có các biện pháp phòng, chống các thông tin vi phạm pháp luật, ảnh hưởng đến an ninh quốc gia, trật tự, an toàn xã hội trên môi trường mạng, nhất là trên các Cổng/Trang thông tin điện tử, mạng xã hội.

5. Là cơ quan đầu mối thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trên địa bàn thị xã.

Điều 10. Trách nhiệm của Văn phòng HĐND và UBND thị xã

1. Vận hành hệ thống thông tin tại trụ sở HĐND-UBND thị xã và các hệ thống phần cứng, phần mềm thuộc thẩm quyền quản lý đảm bảo theo quy định tại Quy chế này và các nhiệm vụ do UBND thị xã phân công.

2. Chỉ đạo, phân công bộ phận kỹ thuật thuộc đơn vị thực hiện quản lý ứng dụng; quản lý dữ liệu; vận hành hệ thống thông tin; triển khai và hỗ trợ kỹ thuật; triển khai công tác bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin thuộc thẩm quyền được phân công quản lý.

3. Phối hợp với Công an thị xã và Phòng Văn hóa - Thông tin thị xã thực hiện các biện pháp phòng, chống các thông tin vi phạm pháp luật, ảnh hưởng đến an ninh quốc gia, trật tự, an toàn xã hội trên môi trường mạng, nhất là trên các Cổng/Trang thông tin điện tử thị xã.

4. Cử cán bộ tham gia các lớp đào tạo, tập huấn về công tác bảo đảm an toàn thông tin mạng.

Điều 11. Trách nhiệm của Công an thị xã

1. Chủ trì, phối hợp với Phòng Văn hóa - Thông tin thị xã và các cơ quan, đơn vị có liên quan chịu trách nhiệm quản lý, kiểm soát, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống thông tin gây phương hại đến an toàn thông tin mạng trong cơ quan nhà nước.

2. Cử cán bộ phối hợp, tham gia các đoàn kiểm tra, đánh giá công tác đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan, đơn vị; Điều tra và xử lý các trường hợp vi phạm các quy định về an toàn thông tin mạng theo thẩm quyền.

3. Kiểm tra đột xuất các cơ quan, đơn vị khi phát hiện có dấu hiệu vi phạm pháp luật về an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin theo đúng quy định của pháp luật.

Điều 12. Trách nhiệm của Phòng Tài chính – Kế hoạch thị xã

Hàng năm, căn cứ khả năng cân đối ngân sách và chế độ, tiêu chuẩn, định mức do nhà nước ban hành, tham mưu Ủy ban nhân dân thị xã bố trí kinh phí triển khai thực hiện nhiệm vụ chuyên môn về bảo đảm an toàn thông tin theo phân cấp hiện hành của Luật Ngân sách Nhà nước.

Điều 13. Trách nhiệm của các cơ quan, đơn vị và UBND các xã, phường

1. Thủ trưởng các cơ quan, đơn vị; Chủ tịch UBND các xã, phường có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trong công tác bảo đảm an toàn thông tin mạng của cơ quan, đơn vị mình; quản lý theo quy định tại Luật An toàn thông tin mạng và các văn bản hướng dẫn thi hành Luật An toàn thông tin mạng.

2. Phân công cán bộ thực hiện việc bảo đảm an toàn thông tin của cơ quan, đơn vị; chỉ đạo công chức, viên chức và người lao động nghiêm túc chấp hành các quy định về bảo đảm an toàn thông tin; thường xuyên tổ chức quán triệt các quy định về an toàn thông tin trong cơ quan, đơn vị.

3. Thực hiện bảo đảm an toàn thông tin gồm các nội dung cơ bản như quy định về quản lý hạ tầng mạng, bảo đảm an toàn dữ liệu, bảo đảm an toàn thiết bị và người dùng đầu cuối phù hợp với Quy chế này và các quy định của pháp luật.

4. Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố xảy ra một cách kịp thời, nhanh chóng và đạt hiệu quả.

5. Phối hợp chặt chẽ với Công an thị xã, Phòng Văn hóa - Thông tin thị xã và các cơ quan, đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin trên không gian mạng.

6. Hàng năm bố trí 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 cơ quan, đơn vị mình.

7. Phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin.

8. Thực hiện các báo cáo về an toàn thông tin mạng khi UBND thị xã có yêu cầu.

Điều 14. Trách nhiệm của các doanh nghiệp cung cấp dịch vụ viễn thông, CNTT và Internet cho các cơ quan quản lý nhà nước trên địa bàn thị xã

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 toàn thông tin và các nội dung quy định tại Quy chế này.

2. Phối hợp với Phòng Văn hóa - Thông tin thị xã 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 sử dụng dịch vụ.

3. Đảm bảo đúng trách nhiệm hợp đồng cung cấp dịch vụ mạng cho các cơ quan, đơn vị được thông suốt, ổn định.

4. Chịu hoàn toàn trách nhiệm nếu có sự cố xảy ra mà thời gian xử lý vượt quá 4 giờ kể từ thời điểm nhận được thông tin sự cố.

5. Chịu hoàn toàn trách nhiệm về chất lượng dịch vụ nếu để số sự cố xảy ra quá 3 lần/tháng/01 đơn vị.

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

1. Trách nhiệm của cán bộ phụ trách về an toàn thông tin/công nghệ thông tin tại cơ quan, đơn vị

a) Chịu trách nhiệm bảo đảm an toàn thông tin mạng của cơ quan, đơn vị;

b) Tham mưu lãnh đạo cơ quan ban hành các quy chế, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin mạng;

c) Thực hiện việc giám sát, đánh giá, báo cáo Thủ trưởng cơ quan, đơn vị các rủi ro mất an toàn thông tin mạng và mức độ nghiêm trọng của các rủi ro đó;

d) Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn thông tin mạng;

đ) Thường xuyên cập nhật nâng cao kiến thức, trình độ chuyên môn đáp ứng yêu cầu bảo đảm an toàn thông tin mạng của đơn vị.

2. Trách nhiệm của người sử dụng

a) 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. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao;

b) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng;

c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý;

d) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được đơn vị chuyên môn tổ chức.

Điều 16. Trách nhiệm của các tổ chức, cá nhân liên quan

1. Các tổ chức, cá nhân khác có sử dụng các hệ thống thông tin do Ủy ban nhân dân thị xã triển khai hoặc liên quan đến hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước của thị xã phải tuân thủ Quy chế này và các quy định hiện hành của pháp luật có liên quan.

2. Khi phát hiện sự cố ảnh hưởng đến an toàn hệ thống thông tin, phải thông báo ngay với cơ quan Nhà nước, nơi tổ chức, cá nhân đang thực hiện giao tiếp.

3. Các tổ chức, cá nhân tham gia vào quá trình ứng dụng công nghệ thông tin trên địa bàn thị xã, chịu sự thanh tra, kiểm tra của các cơ quan Nhà nước có thẩm quyền về lĩnh vực an toàn thông tin.

Điều 17. Tổ chức thực hiện

1. Căn cứ Quy chế này, thủ trưởng các cơ quan, đơn vị trên địa bàn thị xã và các đơn vị, cá nhân liên quan có trách nhiệm tổ chức triển khai thực hiện Quy chế này trong phạm vi quản lý của mình.

2. Phòng Văn hóa - Thông tin thị xã có trách nhiệm theo dõi, đôn đốc, kiểm tra, đánh giá việc thực hiện Quy chế, báo cáo Ủy ban nhân dân thị xã theo định kỳ hằng năm hoặc đột xuất theo yêu cầu của UBND thị xã và cơ quan có thẩm quyền.

3. Trong quá trình thực hiện Quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời về Phòng Văn hóa - Thông tin thị xã để tổng hợp, báo cáo Ủy ban nhân dân thị xã xem xét điều chỉnh, bổ sung./.