ỦY BAN NHÂN DÂN PHƯỜNG BẠCH SAM	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 69 /QĐ-UBND	*Bạch Sam, ngày 22 tháng 5 năm 2024*

QUYẾT ĐỊNH

Về việc ban hành Quy chế Đảm bảo an toàn, an ninh thông tin mạng trong hoạt động của các cơ quan Nhà nước trên địa bàn phường Bạch Sam

ỦY BAN NHÂN DÂN PHƯỜNG BẠCH SAM

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19/6/2015; 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 Công nghệ thông tin ngày 26 tháng 6 năm 2016;

Căn cứ Luật Giao dịch điện tử ngày 22 tháng 6 năm 2023;

Căn cứ Quyết định số 05/2016/QĐ-UBND ngày 17/3/2016 của UBND tỉnh Hưng Yên về việc Ban hành Quy chế 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 Hưng Yên;

Căn cứ Quyết định số 2085/QĐ-UBND ngày 24/4/2024 của UBND thị xã Mỹ Hào về việc Ban hành Quy chế 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 thị xã Mỹ Hào;

Theo đề nghị của Công chức Văn hóa xã hội phường,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn, an ninh thông tin mạng trong hoạt động của các cơ quan Nhà nước trên địa bàn phường Bạch Sam (*có Quy chế kèm theo*).

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

Điều 3. Văn phòng thống kê UBND phường, Công chức Văn hóa xã hội phường, Trưởng các ngành, đoàn thể, CBCC phường, các tổ dân phố chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Phòng VHTT thị xã;
- TT Đảng ủy, HĐND phường;
- Chủ tịch, Phó chủ tịch UBND phường;
- Lưu: VP, VHXH.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Ký bởi: Ủy ban nhân dân phường Bạch Sam
Cơ quan: Tỉnh Hưng Yên
Thời gian ký: 22/05/2024 17:31:37

Đào Trường Giang

ỦY BAN NHÂN DÂN **PHƯỜNG BẠCH SAM**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**

QUY CHẾ
Đảm bảo an toàn, an ninh thông tin mạng trong hoạt động của các cơ quan Nhà nước trên địa bàn phường Bạch Sam

(Ban hành kèm theo Quyết định số: /QĐ-UBND ngày tháng năm 2024 của UBND phường Bạch Sam)

CHƯƠNG I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi áp dụng

Quy chế này quy định về công tác Đảm bảo an toàn, an ninh thông tin mạng trong hoạt động của các cơ quan Nhà nước trên địa bàn phường Bạch Sam.

Điều 2. Đối tượng áp dụng

Quy chế này áp dụng đối với cán bộ, công chức, viên chức, người lao động tại các ngành, đoàn thể phường, các tổ dân phố trên địa bàn phường trong việc quản lý, khai thác, sử dụng và đảm bảo an toàn, an ninh thông tin mạng nhằm phục vụ công tác chuyên môn.

Điều 3. Mục đích, nguyên tắc đảm bảo an toàn, an ninh thông tin

1. Các ngành, đoàn thể, cá nhân có trách nhiệm bảo đảm an toàn, an ninh thông tin mạng. Hoạt động an toàn thông tin mạng của ngành, đoàn thể, 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 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 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.

Điều 4. Giải thích từ ngữ

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

1. An toàn thông tin mạng là công tác bảo vệ thông tin, hệ thống thông tin trên mạng 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.

2. Hệ thống thông tin là tập hợp 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 trên mạng của một cơ quan, tổ chức.

3. Chủ quản hệ thống thông tin là cơ quan tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin.

4. Đơn vị vận hành hệ thống thông tin là cơ quan, tổ chức được chủ quản hệ thống thông tin giao nhiệm vụ vận hành hệ thống thông tin. Trong trường hợp chủ quản hệ thống thông tin thuê ngoài dịch vụ công nghệ thông tin, đơn vị vận hành hệ thống thông tin là bên cung cấp dịch vụ.

5. Sự cố an toàn thông tin mạng là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

6. 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.

7. Mạng ngang hàng là mô hình mạng mà trong đó các máy tính có quyền bình đẳng như nhau, mỗi máy tính có quyền chia sẻ tài nguyên và sử dụng các tài nguyên từ máy tính khác.

8. Cán bộ chuyên trách/cán bộ phụ trách là cán bộ, công chức, viên chức, người lao động được tuyển dụng phụ trách an toàn thông tin/công nghệ thông tin tại các cơ quan, đơn vị, địa phương.

CHƯƠNG II
QUY ĐỊNH ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 5. Bảo vệ bí mật Nhà nước trong hoạt động ứng dụng CNTT

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

a) Không được sử dụng máy tính nối mạng Internet để soạn thảo văn bản; chuyển giao, lưu trữ thông tin có nội dung thuộc bí mật Nhà nước; cung cấp tin, tài liệu và đưa thông tin bí mật Nhà nước trên Cổng/Trang Thông tin điện tử.

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 vi 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, địa phương 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/phụ trách phải dùng các biện pháp kỹ thuật xóa bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

Điều 6. Quy định về cấp phát thu hồi cập nhật và quản lý các tài khoản truy cập vào hệ thống thông tin

1. 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, phải có cơ chế xác định các cá nhân, đơn vị 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.

2. Cán bộ chuyên trách/phụ trách thực hiện quản lý, cấp tài khoản cá nhân hướng dẫn người sử dụng thay đổi mật khẩu ngay sau khi đăng nhập lần đầu tiên và bảo vệ thông tin của tài khoản theo quy định.

3. 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 đặc biệt như !.@,#,$,%...).

Điều 7. Bảo đảm an toàn hạ tầng mạng

1. Quản lý hạ tầng mạng nội bộ

a) Thiết bị CNTT được trang bị tại các ngành, đoàn thể phường là tài sản Nhà nước, được quản lý, sử dụng theo quy định của Nhà nước. Các ngành, đoàn thể, cán bộ, công chức, viên chức và người lao động có trách nhiệm quản lý trang thiết bị được giao.

b) Giao Văn phòng thống kê UBND phường làm công tác quản trị mạng, trực tiếp quản lý kỹ thuật và duy trì hoạt động của các hệ thống thông tin của phường; là đầu mối kết nối mạng LAN, mạng Internet, mạng dữ liệu chuyên dùng cho các bộ phận chuyên môn; kiểm tra hiện trạng, đề xuất sửa chữa hoặc mua mới các chủng loại thiết bị CNTT phù hợp, an toàn, bảo mật theo quy định về quản lý, sử dụng tài sản của cơ quan.

c) Các ngành, đoàn thể thực hiện phân công nhiệm vụ cho cán bộ công chức phụ trách công tác đảm bảo an toàn, an ninh thông tin của ngành, đoàn thể mình; phối hợp với Văn phòng thống kê UBND phường, công chức Văn hóa xã hội và các cơ quan có thẩm quyền khác trong đảm bảo công tác an toàn, an ninh mạng.

2. Quản lý hệ thống mạng không dây

a) Khi thiết lập mạng không dây để kết nối với mạng cục bộ thông qua các điểm truy nhập, các ngành, đoàn thể phải thiết lập các tham số: Tên, nhận dạng dịch vụ, mật khẩu 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 đặc biệt như: !,@,#,$,%), cấp phép truy nhập đối với địa chỉ vật lý, mã hóa dữ liệu theo cơ chế bảo mật WPA2 hoặc WPA3.

b) Mật khẩu đăng nhập phải được thiết lập có độ phức tạp cao, định kỳ 6 tháng thay đổi mật khẩu nhằm tăng cường công tác bảo mật.

Điều 8. Bảo đảm an toàn dữ liệu

1. Quản lý tài khoản và chữ ký số

a) Khi được cấp tài khoản, chữ ký số lần đầu cán bộ, công chức, viên chức phải thay đổi mật khẩu sau khi đăng nhập thành công lần đầu.

b) Các hệ thống thông tin khi phân quyền phải thiết lập chế độ giới hạn số lần đăng nhập không hợp lệ vào hệ thống tối đa không quá 05 lần, khi người dùng đăng nhập sai vượt quá số lần quy định, tài khoản chuyển sang chế độ khóa quyền truy cập.

c) Chủ tài khoản, chữ ký số không chia sẻ, giao quyền tài khoản, chữ ký số và mật khẩu truy nhập cho người khác. Không sử dụng tài khoản của người khác (ví dụ tài khoản phần mềm Quản lý văn bản và Điều hành, Một cửa điện tử…) để đăng nhập vào hệ thống thông tin, cơ sở dữ liệu.

d) Tài khoản thư công vụ và chữ ký số do Ban Cơ yếu Chính phủ cấp để phục vụ cho các hoạt động mang tính công vụ, không sử dụng để giao dịch, đăng ký trên mạng xã hội, các trang mạng xã hội khác.

đ) Tài khoản quản trị hệ thống được giao cho cán bộ chuyên trách/cán bộ phụ trách phục vụ cho công tác quản trị, phân quyền, cấu hình hệ thống đó. Không sử dụng cùng một mật khẩu cho nhiều tài khoản khác nhau.

e) Khi cá nhân thay đổi vị trí công tác, thôi việc, nghỉ hưu…ngay từ thời điểm Quyết định có hiệu lực, các ngành, đoàn thể quản lý cá nhân đó phải báo cáo bằng văn bản cho bộ phận vận hành để điều chỉnh, thu hồi, hủy bỏ tài khoản.

2. Khi thực hiện chia sẻ tài nguyên trên máy tính, các cá nhân, phải sử dụng mật khẩu để bảo vệ thông tin, dữ liệu; không thực hiện chia sẻ toàn bộ ổ cứng; theo dõi, giám sát để kết thúc chia sẻ tài nguyên ngay khi hoàn thành. Các thông tin, tài liệu, dữ liệu nhạy cảm phải được mã hóa trước khi trao đổi, truyền nhận qua mạng máy tính.

3. Cá nhân sử dụng máy tính và thiết bị lưu trữ khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài cơ quan, phải tháo rời bộ phận lưu trữ khỏi thiết bị và để lại cơ quan, hoặc xóa dữ liệu lưu trữ trên thiết bị. Khi thanh lý thiết bị phải xóa dữ liệu lưu trữ bằng phần mềm hoặc thiết bị hủy dữ liệu chuyên dụng.

4. Thông tin, dữ liệu thuộc phạm vi bí mật Nhà nước phải được quản lý theo quy định hiện hành về bảo vệ bí mật Nhà nước.

CHƯƠNG III
TRÁCH NHIỆM SỬ DỤNG VÀ TỔ CHỨC THỰC HIỆN

Điều 9. Bảo đảm an toàn máy tính cá nhân, bảo mật cơ sở dữ liệu và an ninh mạng

1. Văn phòng thống kê UBND phường thực hiện cài đặt, quản lý các phần mềm hệ thống và phần mềm ứng dụng trong hệ thống mạng máy tính tại các bộ phận chuyên môn thuộc UBND phường; nghiên cứu, đề xuất nâng cấp công nghệ, phần mềm theo định hướng quản lý Nhà nước và cơ quan có thẩm quyền.

2. Bảo mật số liệu: Cán bộ, công chức, viên chức, người lao động phải có trách nhiệm bảo mật số liệu trên máy tính.

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

4. Bảo 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 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.

5. An toàn trong sử dụng: Khi không làm việc với máy vi tính trong thời gian dài, cán bộ, công chức, viên chức, người lao động phải tắt máy tính hoặc đặt chế độ bảo vệ để đảm bảo an toàn cho dữ liệu của cá nhân.

6. Phòng, chống virus: Cán bộ, công chức, viên chức, người lao động 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 cho 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.

Điều 10. Trách nhiệm của các ngành, đoàn thể.

1. Trưởng các ngành, đoàn thể có trách nhiệm tổ chức triển khai thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước Chủ tịch UBND phường trong công tác đảm bảo an toàn thông tin của ngành mình.

2. Ưu tiên nguồn kinh phí thường xuyên cho việc triển khai các biện pháp đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của phường. Chủ động bố trí hạng mục an toàn thông tin khi xây dựng Kế hoạch thực hiện chuyển đổi số hằng năm; đảm bảo tỷ lệ chi cho các sản phẩm, dịch vụ an toàn thông tin mạng tối thiểu đạt 10% trên tổng kinh phí dự kiến.

3. Khi xảy ra sự cố hoặc nguy cơ mất an toàn thông tin phải kịp thời áp dụng mọi biện pháp để khắc phục và hạn chế mức thấp nhất thiệt hại có thể xảy ra; thông báo cho cơ quan có thẩm quyền để phối hợp, xử lý.

5. Phối hợp với Văn phòng thống kê UBND phường và các bọ phận liên quan thực hiện công tác kiểm tra, khắc phục sự cố nhanh chóng, kịp thời và hiệu quả; đồng thời cung cấp đầy đủ thông tin khi được yêu cầu.

6. Phối hợp chặt chẽ với cơ quan Công an trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn, an ninh thông tin. Tạo điều kiện thuận lợi cho các cơ quan chức năng tham gia khắc phục sự cố và thực hiện đúng theo hướng dẫn.

7. Định kỳ hàng năm báo cáo tình hình, kết quả thực hiện công tác đảm bảo an toàn, an ninh thông tin gửi về UBND phường trước ngày 15 tháng 11 để tổng hợp, báo cáo UBND thị xã.

Điều 11. Trách nhiệm của Văn phòng thống kê UBND phường

1. Chủ trì, phối hợp với công chức Văn hóa xã hội, các ngành, đoàn thể liên quan triển khai thực hiện các biện pháp bảo đảm an toàn an ninh mạng đối với hệ thống thông tin đang được sử dụng tại các bộ phận trên địa bàn phường.

2. Đảm bảo duy trì kết nối với mạng Truyền số liệu chuyên dùng và Nền tảng giám sát an toàn thông tin mạng (SOC) của tỉnh để kịp thời phát hiện, khắc phục sự cố về an toàn an ninh mạng.

3. Là bộ phận đầu mối về ứng cứu sự cố máy tính của phường, tham gia vào mạng lưới điều phối ứng cứu sự cố của thị xã, tiếp nhận và xử lý các thông báo sự cố về an toàn thông tin. Tùy theo mức độ sự cố, phối hợp với công chức Văn hóa xã hội, Phòng Văn hoá Thông tin thị xã, các đơn vị có liên quan hướng dẫn xử lý, ứng cứu sự cố mất an toàn thông tin.

Điều 12. Trách nhiệm của công chức Văn hóa xã hội

1. Tham mưu UBND phường về công tác đảm bảo an toàn, an ninh thông tin; bố trí hạng mục và an toàn thông tin khi xây dựng Kế hoạch thực hiện chuyển đổi số hàng năm, đảm bảo tỷ lệ chi cho các sản phẩm, dịch vụ an toàn thông tin mạng tối thiểu đạt 10% trên tổng kinh phí dự kiến.

2. Là bộ phận đầu mối về ứng cứu sự cố máy tính của phường, tham gia vào mạng lưới điều phối ứng cứu sự cố của thị xã, tiếp nhận và xử lý các thông báo sự cố về an toàn thông tin. Phối hợp với Văn phòng thống kê UBND phường, Phòng Văn hoá thông tin thị xã, các đơn vị có liên quan hướng dẫn xử lý, ứng cứu sự cố mất an toàn thông tin.

3. Chủ trì, phối hợp với các bộ phận liên quan tổ chức kiểm tra theo định kỳ hoặc kiểm tra đột xuất công tác đảm bảo an toàn thông tin khi phát hiện có các dấu hiệu, hành vi vi phạm an toàn thông tin.

4. Tổ chức tuyên truyền, hướng dẫn, đôn đốc các hoạt động liên quan đến công tác đảm bảo an toàn an ninh mạng để thúc đẩy việc triển khai đồng bộ, toàn diện công tác đảm bảo an toàn thông tin mạng tại các ngành, đoàn thể trên địa bàn phường.

5. Tổng hợp, báo cáo tình hình đảm bảo an toàn thông tin theo định kỳ, gửi Phòng Văn hoá thông tin, UBND thị xã và các cơ quan có liên quan.

Điều 13. Trách nhiệm của Công an phường

1. Phối hợp với Công chức Văn hóa xã hội, Văn phòng thống kê UBND phường và các cơ quan liên quan kiểm tra công tác đảm bảo an toàn, an ninh thông tin.

2. Tham mưu xây dựng kế hoạch về phòng, chống tội phạm và vi phạm pháp luật khác về an toàn, an ninh thông tin.

3. Thường xuyên thông báo cho các ngành, đoàn thể, CBCC về phương thức, thủ đoạn của các loại tội phạm xâm phạm an toàn, an ninh thông tin để có biện pháp phòng ngừa, phát hiện, đấu tranh, ngăn chặn.

4. Hướng dẫn các ngành, đoàn thể, CBCC phòng, chống, ngăn ngừa và đấu tranh với các hành vi vi phạm pháp luật khác về an toàn, an ninh thông tin.

5. Điều tra, xử lý các các trường hợp vi phạm pháp luật về an toàn, an ninh thông tin theo thẩm quyền.

Điều 14. Trách nhiệm của cán bộ, công chức, viên chức, người lao động khi tham gia sử dụng và khai thác hệ thống thông tin

1. Nghiêm chỉnh thực hiện các nội quy, quy chế, quy trình về bảo đảm an toàn thông tin, an ninh mạng của phường cũng quy định khác của pháp luật về nội dung này.

2. Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo kịp thời cho cán bộ chuyên trách/phụ trách công nghệ thông tin của phường mình để kịp thời ngăn chặn và xử lý.

3. Nâng cao ý thức cảnh giác và trách nhiệm về an toàn thông tin, an ninh mạng. Không được truy cập vào các liên kết (link) không rõ ràng; không sử dụng địa chỉ thư điện tử công vụ vào mục đích cá nhân như: đăng ký tài khoản mạng xã hội, đăng ký mua sắm qua mạng.

4. Không sử dụng các hộp thư điện tử miễn phí Gmail, Yahoo,…trong hoạt động công vụ và tại máy tính có nối mạng ở phòng, ngành, đoàn thể mình nhằm đảm bảo an toàn thông tin trên môi trường mạng.

5. Cá nhân sử dụng các thiết bị lưu trữ di động (máy tính xách tay, thiết bị số cầm tay, thẻ nhớ USB, ổ cứng di động, băng từ..) để lưu thông tin thuộc danh mục bí mật Nhà nước có trách nhiệm bảo vệ các thiết bị này và thông tin trên thiết bị, tránh làm mất, lộ thông tin. Nghiêm cấm việc bán, cho mượn, giao người không có trách nhiệm sử dụng thiết bị do cá nhân tự trang bị có lưu giữ bí mật Nhà nước.

6. Không được lợi dụng việc sử dụng Internet nhằm mục đích: Chống lại Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội; kích động bạo lực, đồi trụy, tệ nạn xã hội, mê tín dị đoan; phá hoại thuần phong mỹ tục của dân tộc; không được truy cập hoặc tải các trang Website có nội dung đồi trụy, phản động, các chương trình không rõ nguồn gốc, các thông tin quảng cáo hấp dẫn.

7. Không chơi các trò chơi trực tuyến (online) hoặc các trò chơi khác trên Internet trong giờ làm việc.

8. Khi sử dụng thư điện tử công vụ không được kích chuột vào bất cứ thư điện tử, tệp đính kèm, đường link, thư rác, thư quảng cáo không rõ nguồn gốc và không xác định được người gửi.

9. Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin phải báo cáo ngay với cấp trên, phối hợp với công chức Văn hóa xã hội, Văn phòng thống kê UBND phường để kịp thời ngăn chặn, xử lý.

10. Tham gia các chương trình đào tạo, tập huấn, hội nghị về an toàn, an ninh thông tin do Sở Thông tin và Truyền thông hoặc các cơ quan, đơn vị chuyên môn tổ chức.

Điều 15. Khen thưởng và xử lý vi phạm

1. Hàng năm, công chức Văn hóa xã hội căn cứ báo cáo về công tác an toàn, an ninh thông tin của các ngành, đoàn thể để tổ chức, đánh giá thực hiện an toàn, an ninh thông tin; trên cơ sở đó đề xuất UBND các cấp khen thưởng theo quy định hiện hành.

2. Các ngành, đoàn thể, cá nhân có hành vi vi phạm Quy chế này tùy theo tính chất, mức độ vi phạm mà xử lý theo quy định của pháp luật.

Điều 16. Điều khoản thi hành

Công chức Văn hóa xã hội có trách nhiệm chủ trì, phối hợp với các ngành, bộ phận chuyên môn có liên quan hướng dẫn, triển khai và kiểm tra, đôn đốc việc thực hiện Quy chế này.

Trong quá trình thực hiện Quy chế này, nếu có vướng mắc, đề nghị các ngành, đoàn thể, CBCC, các booh phận có liên quan gửi văn bản về UBND phường (qua công chức Văn hóa xã hội) để tổng hợp, báo cáo Uỷ ban nhân dân phường xem xét, sửa đổi, bổ sung cho phù hợp./.