|  |  |
| --- | --- |
| **ỦY BAN NHÂN DÂN   XÃ ÔNG ĐÌNH** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc** |
| Số: 253 /QĐ-UBND | *Ông Đình, ngày 11 tháng 9 năm 2024* |

**QUYẾT ĐỊNH**

**Về việc ban hành Quy định đảm bảo an toàn, an ninh thông tin**

**trên môi trường mạng trong hoạt động của các cơ quan nhà nước**

**trên địa bàn xã Ông Đình**

**ỦY BAN NHÂN DÂN XÃ ÔNG ĐÌNH**

*Căn cứ Luật tổ chức Chính quyền địa phương ngày 19/6/2015;*

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

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

*Căn cứ Nghị định số* [*64/2007/NĐ-CP*](http://thuvienphapluat.vn/phap-luat/tim-van-ban.aspx?keyword=64/2007/N%C4%90-CP&area=2&type=0&match=False&vc=True&lan=1) *ngày 10/4/2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước; Nghị định số* [*72/2013/NĐ-CP*](http://thuvienphapluat.vn/phap-luat/tim-van-ban.aspx?keyword=72/2013/N%C4%90-CP&area=2&type=0&match=False&vc=True&lan=1) *ngày 15/07/2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng;*

*Căn cứ Chỉ thị số* [*15/CT-TTg*](http://thuvienphapluat.vn/phap-luat/tim-van-ban.aspx?keyword=15/CT-TTg&area=2&type=0&match=False&vc=True&lan=1) *ngày 17/6/2014 của Thủ tướng Chính phủ tăng cường công tác đảm bảo an ninh và an toàn thông tin mạng trong tình hình mới;*

*Căn cứ Quyết định số 05/2016/QĐ-UBND ngày 17/3/2016 của UBND tỉnh về 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 2128/QĐ-UBND ngày 28/4/2017 của UBND huyện về việc ban hành quy định 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 huyện Khoái Châu.*

*Theo đề nghị của Công chức Văn phòng thống kê UBND xã.*

**QUYẾT ĐỊNH:**

**Điều 1.** Ban hành kèm theo Quyết định này Quy định đảm bảo an toàn, an ninh thông tin trên môi trường mạng trong hoạt động của các cơ quan nhà nước trên địa bàn xã Ông Đình,

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

**Điều 3.** Công chức Văn phòng thống kê UBND xã, Tài chính kế toán, các ban ngành đoàn thể các thôn, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

|  |  |
| --- | --- |
| ***Nơi nhận:***  - Như Điều 3;  - UBND huyện;  - Thường trực Đảng ủy;  - Thường trực HĐND xã;  - Chủ tịch, các PCT UBND xã;  - Công an xã; VP, VH-XH  - Lưu VT | **TM. ỦY BAN NHÂN DÂN CHỦ TỊCH**    **Nguyễn Duy Định** |

**QUY ĐỊNH**

**Đảm bảo an toàn, an ninh thông tin trên môi trường mạng trong**

**hoạt động của các cơ quan nhà nước trên địa bàn xã Ông Đình**

*(Ban hành kèm theo Quyết định số 253 /QĐ-UBND ngày 11/9/2024*

*của UBND xã Ông Đình)*

**Chương I**

**QUY ĐỊNH CHUNG**

**Điều 1. Phạm vi điều chỉnh**

1. Quy định về việc đảm bảo an toàn, an ninh thông tin trên môi trường mạng trong hoạt động của các cơ quan nhà nước trên địa bàn xã Chí Tân bao gồm: Công tác quản lý đảm bảo an toàn, an ninh thông tin mạng; việc áp dụng các biện pháp quản lý kỹ thuật, quản lý vận hành đảm bảo an toàn, an ninh thông tin đối với các hệ thống thông tin.

2. Đối với lực lượng vũ trang ngoài việc thực hiện theo quy định chung còn thực hiện theo quy định riêng của ngành trong đảm bảo an ninh thông tin, bảo mật trên môi trường mạng.

**Điều 2. Đối tượng áp dụng**

1. Quy định này được áp dụng đối với các cơ quan nhà nước trên địa bàn xã Chí Tân bao gồm: Các bộ phận, cơ quan chuyên môn thuộc Ủy ban nhân dân xã và các ban ngành đoàn thể xã (sau đây gọi tắt là cơ quan, đơn vị).

2. Cán bộ, công chức, viên chức đang làm việc trong các cơ quan, đơn vị nêu tại Khoản 1 Điều này và những cá nhân, tổ chức có liên quan áp dụng Quy định này trong việc vận hành, khai thác hệ thống thông tin tại các cơ quan, đơn vị.

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

1. Việc áp dụng Quy chế này nhằm giảm thiểu được các nguy cơ gây mất an toàn thông tin và đảm bảo an ninh thông tin trong quá trình ứng dụng công nghệ thông tin trong hoạt động của các cơ quan.
2. Các hoạt động ứng dụng công nghệ thông tin phải tuân theo nguyên tắc đảm bảo an toàn thông tin được quy định tại Điều 41, Nghị định 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.
3. Công tác đảm bảo an toàn, an ninh thông tin, bảo mật trên môi trường mạng là nhiệm vụ trọng tâm để xây dựng Công sở điện tử hướng đến Chính quyền điện tử, Chính quyền số đảm bảo triển khai thành công trong việc ứng dụng công nghệ thông tin trong hoạt động của các cơ quan nhà nước.

**Điều 4. Giải thích từ ngữ**

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

1. An toàn thông tin số: Là thuật ngữ dùng để chỉ việc bảo vệ thông tin số và các hệ thống thông tin chống lại các nguy cơ tự nhiên, các hành động truy cập, sử dụng, phát tán, phá hoại, sửa đổi và phá hủy bất hợp pháp nhằm bảo đảm cho các hệ thống thông tin thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy. Nội dung của an toàn thông tin mạng bao gồm bảo vệ an toàn mạng và hạ tầng thông tin, an toàn máy tính, dữ liệu và ứng dụng và dịch vụ công nghệ thông tin.

2. Hệ thống thông tin: là một tập hợp và kết hợp các phần cứng, phần mềm, các hệ thống mạng truyền thông được xây dựng và sử dụng để thu thập, tạo, tái tạo, phân phối và chia sẻ các dữ liệu, thông tin, tri thức nhằm phục vụ cho các mục tiêu của tổ chức.

3. An toàn, an ninh thông tin: Là đảm bảo thông tin được bảo mật, sẵn sàng và toàn vẹn.

4. Tính tin cậy: Là đảm bảo thông tin chỉ có thể được truy cập bởi những người được cấp quyền truy cập.

5. Tính toàn vẹn: Là bảo vệ tính chính xác, tính đầy đủ của thông tin và các phương pháp xử lý thông tin.

6. Tính sẵn sàng: Là đảm bảo những người được cấp quyền có thể truy cập thông tin và các tài liệu có liên quan ngay khi có nhu cầu.

7. Môi trường mạng bao gồm: Mạng nội bộ (LAN); mạng diện rộng của Ủy ban nhân dân xã, của ngành (WAN); mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước; mạng riêng ảo (VPN), mạng Intranet; mạng Internet.

8. TCVN 7562:2005: Tiêu chuẩn Việt Nam về mã thực hành quản lý an toàn thông tin.

9. TCVN ISO/IEC 27001:2009: Tiêu chuẩn Việt Nam về quản lý an toàn thông tin số.

**Điều 5. Các hành vi bị nghiêm cấm**

1. Ngăn chặn trái pháp luật việc truyền tải thông tin trên mạng; can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sửa chữa, sao chép, làm sai lệch trái phép thông tin mạng.
2. Cản trở, trái pháp luật hoạt động của hệ thống thông tin, phá hoại cơ sở hạ tầng thông tin, thông tin trên môi trường mạng, gây ảnh hưởng tới khả năng truy nhập hợp pháp của người sử dụng tới hệ thống thông tin.

3. Lợi dụng mạng để tuyên truyền, chống phá Nhà nước Cộng hoà xã hội chủ nghĩa Việt Nam; thực hiện các hành vi gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội; phá hoại khối đại đoàn kết toàn dân.

5. Quảng bá, tuyên truyền, mua bán hàng hóa, dịch vụ bị cấm; truyền bá tác phẩm báo chí, văn học, nghệ thuật, xuất bản phẩm bị cấm.

6. Tiết lộ bí mật nhà nước, bí mật quân sự, an ninh, kinh tế, đối ngoại và những bí mật khác do pháp luật quy định.

**Chương II**

**QUY ĐỊNH ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN**

**Điều 6. Điều kiện đảm bảo thực hiện nhiệm vụ an toàn, an ninh thông tin**

1. Các cơ quan, đơn vị phải phổ biến những kiến thức cơ bản về an toàn, an ninh thông tin cho cán bộ, công chức, viên chức trước khi tham gia sử dụng hệ thống thông tin.

2. Các cơ quan, đơn vị bố trí cán bộ làm công tác chuyên trách về công nghệ thông tin phải có chuyên ngành phù hợp và được đào tạo, bồi dưỡng chuyên môn đối với lĩnh vực an toàn, an ninh thông tin.

3. Xác định và ưu tiên phân bổ kinh phí cần thiết cho các hoạt động liên quan đến việc bảo vệ hệ thống thông tin, thông qua việc đầu tư các thiết bị tường lửa, các chương trình chống thư rác, virus máy tính trên hệ thống máy chủ, máy trạm và các công tác khác liên quan đến việc bảo đảm an toàn, an ninh thông tin.

4. Cán bộ tham gia đoàn kiểm tra công tác đảm bảo an toàn, an ninh thông tin phải được trang bị đầy đủ những kiến thức và được tập huấn hàng năm về công tác đảm bảo an toàn, an ninh thông tin.

5. Các cơ quan, đơn vị phải xây dựng, ban hành quy chế nội bộ về đảm bảo an toàn, an ninh thông tin; phải căn cứ các nội dung của tiêu chuẩn TCVN 7562:2005 và TCVN ISO/IEC 27001:2009 để quy định rõ các vấn đề sau:

a) Mục tiêu, phạm vi và đối tượng áp dụng.

b) Quy định cụ thể quyền và trách nhiệm của từng đối tượng: Lãnh đạo đơn vị, Lãnh đạo cấp phòng, cán bộ chuyên trách về công nghệ thông tin và người sử dụng.

c) Quy định về cấp phát, thu hồi, cập nhật và quản lý các tài khoản truy cập vào hệ thống thông tin phải đảm bảo chặt chẽ, đúng quy định.

d) Quy định về an toàn, an ninh thông tin trên môi trường mạng trong nội bộ.

đ) Cơ chế sao lưu dữ liệu, cơ chế báo cáo và phối hợp khắc phục sự cố.

e) Theo dõi, kiểm tra, thống kê, tổng hợp, báo cáo theo định kỳ và đột xuất.

h) Tổ chức thực hiện.

**Điều 6. Trang thiết bị và hạ tầng công nghệ thông tin**

1. Cấu hình máy chủ phải đủ mạnh để đáp ứng công việc. Máy chủ của cơ quan chỉ dùng để triển khai phần mềm hệ thống, các dữ liệu lưu trữ cần thiết và các phần mềm chống virus, ngoài ra không được cài thêm bất cứ phần mềm khác.

2. Tất cả các máy tính tại cơ quan, đơn vị phải được cài đặt và bảo vệ bởi phần mềm phòng chống virut, phần mềm độc hại.

3. Đối với tài khoản người dùng sử dụng để đăng nhập các hệ thống thông tin, phần mềm ứng dụng, cơ sở dữ liệu các ứng dụng chuyên ngành khác phải thiết lập mật khẩu có mức bảo mật cao, không sử dụng mật khẩu ngắn, mặc định nhằm đảm bảo an toàn, bảo mật thông tin của người dùng.

4. Hệ thống thông tin cần có cơ chế ngăn chặn hoặc hạn chế các sự cố gây ra do tấn công từ chối dịch vụ (DOS, DDOS). Sử dụng thiết bị tường lửa, xây dựng giải pháp phù hợp để có thể ngăn chặn, phòng tránh bị ảnh hưởng trực tiếp và bảo vệ thiết bị, máy chủ.

5. Trường hợp có sự cố máy tính nghiêm trọng vượt quá khả năng khắc phục của đơn vị, phải báo cáo ngay cơ quan cấp trên quản lý trực tiếp, phối hợp với Văn phòng HĐND và UBND huyện, Phòng Văn hoá Thông tin, Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ khắc phục.

6. Trong quá trình đầu tư mua sắm trang thiết bị CNTT, các phần mềm ứng dụng đi kèm cần lưu ý đến xuất xứ hàng hóa để đảm bảo an toàn, an ninh thông tin mạng.

**Điều 7. Quy định về quản trị phần mềm ứng dụng**

Trong quá trình đầu tư, thiết kế, xây dựng, nâng cấp các phần mềm hệ thống, các phần mềm ứng dụng dùng chung trong các cơ quan nhà nước phải đáp ứng yêu cầu quản trị, vận hành đảm bảo an toàn, an ninh thông tin mạng.

1. Quản lý tài nguyên: Cán bộ quản trị mạng có trách nhiệm kiểm tra, giám sát chức năng chia sẻ thông tin; tổ chức cấp phát tài nguyên trên máy chủ theo danh mục, thư mục cho từng phòng/ban; khuyến cáo người dùng cân nhắc việc chia sẻ tài nguyên cục bộ trên máy đang sử dụng, tuyệt đối không được chia sẻ toàn bộ ổ cứng. Khi thực hiện chia sẻ tài nguyên trên máy chủ hoặc trên máy cục bộ phải sử dụng mật khẩu để bảo vệ thông tin.

2. Quản lý đăng nhập hệ thống: Các hệ thống thông tin cần giới hạn số lần đăng nhập vào hệ thống. Hệ thống tự động khoá tài khoản hoặc cô lập tài khoản khi liên tục đăng nhập sai vượt quá số lần quy định. Tổ chức theo dõi, giám sát tất cả các phương tiện đăng nhập từ xa; yêu cầu người sử dụng đặt mật khẩu với độ an toàn cao, giám sát, nhắc nhở, khuyến cáo nên thay đổi mật khẩu thường xuyên.

3. Quản lý tài khoản: Các tài khoản và định danh người dùng trong các hệ thống thông tin, bao gồm: Tạo mới, kích hoạt, sửa đổi và loại bỏ các tài khoản, đồng thời tổ chức kiểm tra các tài khoản của hệ thống thông tin ít nhất 6 tháng/lần thông qua các công cụ của hệ thống. Hủy tài khoản, quyền truy cập hệ thống đối với cán bộ, công chức đã chuyển công tác hoặc thôi việc.

4. Quản lý nhật ký hệ thống (log file): Hệ thống thông tin phải ghi nhận các sự kiện như: Quá trình đăng nhập vào hệ thống, các thao tác cấu hình hệ thống. Thường xuyên kiểm tra, sao lưu các log file theo từng tháng để lưu vết theo dõi, xác định những sự kiện đã xảy ra của hệ thống và hạn chế việc tràn log file gây ảnh ưởng đến hoạt động của hệ thống.

5. Phòng chống mã độc, virus: Trên các máy chủ, các thiết bị di động trong mạng và hệ thống thông tin phải cài đặt phần mềm chống virus, thư rác phù hợp để phát hiện, loại trừ mã độc, virus và cài đặt các phần mềm này trên máy trạm.

6. Quản lý cài đặt: Cán bộ, công chức, viên chức không được tự ý cài đặt thêm chương trình khác trên máy tính cá nhân nhằm tránh sự lây lan của virus. Cán bộ chuyên trách CNTT có trách nhiệm kiểm tra, cài đặt và chịu trách nhiệm về mức độ an toàn, bảo mật các phần mềm ứng dụng phục vụ công tác chuyên ngành tại các máy tính công vụ của cán bộ, công chức, viên chức.

7. Xung đột phần mềm: Trong quá trình thiết kế, nâng cấp các phần mềm chuyên ngành phải đảm bảo tương thích và tích hợp được với các phần mềm dùng chung đảm bảo tránh được các xung đột và gây mất an toàn 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 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.

2. Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật, các cơ quan phải báo cáo cho cơ quan có thẩm quyền. Không được cho phép các công ty tư nhân hoặc người 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.

**Điều 9. Quản lý, vận hành hệ thống thông tin của đơn vị**

1. Hệ thống thông tin của các cơ quan, đơn vị phải có cơ chế sao lưu dữ liệu ở mức hệ thống, dữ liệu của các ứng dụng, dữ liệu của người sử dụng; cơ chế sao lưu dữ liệu phải được thực hiện thường xuyên; thiết bị lưu trữ dữ liệu được sao lưu phải đảm bảo yêu cầu kỹ thuật; dữ liệu được sao lưu phải đảm bảo tính sẵn sàng và toàn vẹn đáp ứng yêu cầu phục hồi dữ liệu cho hệ thống thông tin hoạt động bình thường khi có sự cố xảy ra.

2. Hệ thống thông tin của các cơ quan, đơn vị phải được triển khai cơ chế bảo mật, an toàn thông tin bằng các thiết bị phần cứng và phần mềm phù hợp với quy mô của đơn vị.

3. Hệ thống thông tin của đơn vị phải được triển khai chức năng giám sát truy cập từ ngoài vào hệ thống, từ hệ thống gửi ra bên ngoài; ghi lại nhật ký (log file) ra, vào hệ thống để phục vụ công tác khắc phục sự cố, điều tra, phân tích và làm rõ các nguy cơ gây ra mất an toàn, an ninh thông tin; chức năng không cho người dùng truy cập một số website không phù hợp với quy định hiện hành.

4. Hệ thống mạng không dây (wireless) của các cơ quan, đơn vị phải được thiết lập khoá khi truy cập tối thiểu 8 ký tự.

5. Mạng riêng ảo (VPN) của các cơ quan, đơn vị kết nối để truy cập vào hệ thống thông tin phải được bảo mật; quản lý và kiểm soát chặt chẽ các kết nối; hủy bỏ kết nối khi không còn sử dụng.

6. Tất cả các tài khoản truy cập vào hệ thống máy chủ, thiết bị mạng, máy tính, các ứng dụng phải được thiết lập mật khẩu; mật khẩu phải được đặt ở mức bảo mật cao (số lượng ký tự và nội dung của mật khẩu); mật khẩu có tối thiểu 6 ký tự bao gồm chữ hoa, chữ thường, chữ số và ký tự đặc biệt; phải thường xuyên thay đổi mật khẩu với tần suất phù hợp; danh sách tài khoản phải được quản lý, kiểm tra và cập nhật kịp thời; quyền truy cập của tài khoản phải được thiết lập phù hợp cho từng đối tượng.

**Điều 10. Cán bộ phụ trách về công nghệ thông tin của đơn vị**

1. Được đảm bảo điều kiện về đào tạo, bồi dưỡng, học tập, nghiên cứu, tiếp thu kiến thức, kỹ thuật và công nghệ mới đối với lĩnh vực an toàn, an ninh thông tin.

2. Quản lý chặt chẽ việc di chuyển các trang thiết bị công nghệ thông tin lưu trữ các thông tin thuộc danh mục bí mật nhà nước.

3. Thực hiện cấp phát, thu hồi, cập nhật và quản lý tất cả các tài khoản truy cập vào hệ thống thông tin của đơn vị; hướng dẫn người sử dụng thay đổi mật khẩu ngay sau khi đăng nhập lần đầu tiên; bảo vệ thông tin của tài khoản theo quy định.

4. Triển khai áp dụng các giải pháp tổng thể đảm bảo an toàn, an ninh thông tin mạng trong toàn hệ thống; triển khai các giải pháp kỹ thuật phòng chống virus, mã độc hại, thư rác cho hệ thống và máy tính cá nhân; kiểm soát và có giải pháp kỹ thuật chống truy cập trái phép vào hệ thống thông tin.

5. Thường xuyên cập nhật các bản vá lỗi đối với hệ thống, cập nhật các phiên bản mới đối với chương trình chống virus.

6. Thường xuyên sao lưu dữ liệu theo quy định; kiểm tra dữ liệu sao lưu phải đảm bảo tính sẵn sàng, tin cậy và toàn vẹn.

7. Thường xuyên thực hiện phân tích, đánh giá và báo cáo các rủi ro và nguy cơ gây mất an toàn, an ninh thông tin đối với hệ thống thông tin của đơn vị; nguyên nhân gây ra các rủi ro và nguy cơ gây mất an toàn, an ninh thông tin mạng bao gồm: Hiện tượng tự nhiên (nhiệt độ, không khí, mưa bão, sét), truy cập trái phép, virus, cố ý làm thay đổi thông số cấu hình hệ thống và phá hủy dữ liệu. Đồng thời tham mưu và xây dựng phương án hạn chế, khắc phục các rủi ro và nguy cơ có thể xảy ra.

**Điều 11. Giải quyết và khắc phục sự cố an toàn, an ninh thông tin**

1. Đối với người sử dụng:

a) Thông tin, báo cáo kịp thời cho cán bộ phụ trách về công nghệ thông tin của cơ quan, đơn vị khi phát hiện các sự cố gây mất an toàn, an ninh thông tin mạng trong quá trình tham gia vào hệ thống thông tin của đơn vị.

b) Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

2. Đối với cán bộ chuyên trách/ phụ trách về công nghệ thông tin:

a) Xử lý khẩn cấp: Khi phát hiện hệ thống nội bộ bị tấn công, thông qua các dấu hiệu như luồng tin (traffic) tăng lên bất ngờ, nội dung bị thay đổi, hệ thống hoạt động chậm bất thường cần thực hiện các bước cơ bản sau:

Bước 1: Ngắt kết nối máy chủ ra khỏi mạng;

Bước 2: Sao chép nhật ký (log file) và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ;

Bước 3: Khôi phục lại hệ thống bằng cách chuyển dữ liệu sao lưu mới nhất để hệ thống hoạt động trở lại bình thường.

Lập biên bản ghi nhận sự cố gây ra mất an toàn, an ninh thông tin đối với hệ thống thông tin của cơ quan, đơn vị; đồng thời thu thập các chứng cứ, dấu vết và nguyên nhân gây ra sự cố (nếu có); đồng thời báo cáo sự cố và kết quả khắc phục sự cố cho Thủ trưởng cơ quan, đơn vị.

b) Trong trường hợp phát hiện sự cố xảy ra ngoài khả năng giải quyết của cơ quan, đơn vị phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp để được hỗ trợ, hướng dẫn và phối hợp khắc phục sự cố; đồng thời tham mưu văn bản báo cáo sự cố gửi Văn phòng thống kê xã, Công an xã và các đơn vị có liên quan.

3. Bộ phận Văn phòng thống kê xã

a) Quyết định toàn diện về mặt kỹ thuật đối với các cơ quan, đơn vị trong quá trình khắc phục sự cố về an toàn, an ninh thông tin.

b) Chỉ đạo các đơn vị trực thuộc nhanh chóng hỗ trợ, phối hợp và hướng dẫn các cơ quan, đơn vị khắc phục sự cố mất an toàn, an ninh thông tin.

c) Yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan, đơn vị nhằm phục vụ công tác khắc phục sự cố về an toàn, an ninh thông tin.

d) Phối hợp với Công an xã trong điều tra làm rõ các nguyên nhân gây ra sự cố mất an toàn, an ninh thông tin.

đ) Trong trường hợp sự cố xảy ra có phạm vi rộng, ảnh hưởng và liên quan đến nhiều ngành, nhiều lĩnh vực phải thông báo khẩn cấp và xin ý kiến chỉ đạo của UBND xã, UBND huyện, Sở Thông tin và Truyền thông.

**Chương III**

**TRÁCH NHIỆM ĐẢM BẢO AN TOÀN,**

**AN NINH THÔNG TIN MẠNG**

**Điều 12. Trách nhiệm của các cơ quan, đơn vị**

1. Thủ trưởng các cơ quan, đơn vị chịu trách nhiệm trước Ủy ban nhân dân xã trong công tác đảm bảo an toàn, an ninh thông tin đối với toàn bộ hệ thống thông tin của đơn vị mình, bao gồm các đơn vị sự nghiệp trực thuộc và các địa phương.

2. Thực hiện và chỉ đạo cán bộ, công chức thuộc thẩm quyền quản lý thực hiện nghiêm túc Quy định này.

3. Tạo điều kiện thuận lợi cho cán bộ chuyên trách về công nghệ thông tin được đào tạo, bồi dưỡng chuyên môn trong lĩnh vực an toàn, an ninh thông tin mạng.

4. Quan tâm đầu tư các thiết bị phần cứng, phần mềm liên quan đến công tác đảm bảo an toàn, an ninh thông tin.

5. Khi có sự cố hoặc nguy cơ mất an toàn, an ninh thông tin mạng phải chỉ đạo khắc phục sự cố kịp thời và hạn chế thấp nhất mức thiệt hại có thể xảy ra, ưu tiên sử dụng lực lượng kỹ thuật tại chỗ của đơn vị mình, đồng thời lập biên bản và báo cáo bằng văn bản cho cơ quan có liên quan.

6. Tạo điều kiện thuận lợi cho các cơ quan chức năng trong công tác điều tra, làm rõ nguyên nhân gây ra sự cố; lực lượng kỹ thuật tham gia khắc phục sự cố thực hiện đúng theo hướng dẫn chuyên môn của Văn phòng thống kê, Phòng Văn hoá và Thông tin, Văn phòng UBND và HĐND huyện.

7. Tổ chức thực hiện ký bản cam kết (nếu cần) cho cán bộ, công chức, viên chức tại đơn vị mình đảm bảo không để lộ, lọt thông tin bí mật nhà nước.

**Điều 13. Trách nhiệm của Văn phòng thống kê xã**

1. Chịu trách nhiệm toàn diện trước Ủy ban nhân dân xã về công tác đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên phạm vi toàn xã.

2. Thực hiện công tác tham mưu Ủy ban nhân dân xã ban hành:

a) Văn bản chỉ đạo, kế hoạch, đề án nhằm đảm bảo an toàn, an ninh thông tin.

b) Xây dựng tiêu chuẩn đánh giá mức độ an toàn, an ninh thông tin đối với hệ thống thông tin của các đơn vị.

c) Xây dựng Danh mục các loại phần mềm được phép triển khai để đảm bảo sử dụng Hạ tầng chùng chung và CSDL tập trung. Danh mục các phần mềm chuyên ngành, phần mềm thương mại được phép cài đặt trên máy tính của cán bộ, công chức, viên chức để đảm bảo an toàn, an ninh thông tin và tiết kiệm ngân sách nhà nước.

d) Xây dựng Quy định danh mục các phần mềm bắt buộc vận hành trong hệ thống mạng WAN của huyện và danh mục những phần mềm có thể triển khai trên hệ thống mạng Internet.

đ) Thành lập đoàn kiểm tra liên ngành về đảm bảo an toàn, an ninh thông tin mạng trong hoạt động ứng dụng công nghệ thông tin trong các cơ quan nhà nước.

3. Hàng năm, tổ chức đào tạo chuyên sâu về an toàn, an ninh thông tin mạng cho lực lượng đảm bảo an toàn, an ninh thông tin mạng của các cơ quan, đơn vị.

4. Thực hiện nhiệm vụ cảnh báo về nguy cơ hoặc sự cố mất an toàn, an ninh thông tin.

5. Tổ chức Hội nghị, Hội thảo chuyên đề về an toàn, an ninh thông tin.

6. Phối hợp với các đơn vị có liên quan trong thực hiện nhiệm vụ đảm bảo an toàn, an ninh thông tin mạng.

7. Phối hợp với Công an xã và các cơ quan, đơn vị có liên quan tổ chức đoàn kiểm tra về an toàn, an ninh thông tin mạng để kịp thời phát hiện, xử lý các hành vi vi phạm theo thẩm quyền quy định.

8. Chủ động hướng dẫn các cơ quan, đơn vị xây dựng quy chế nội bộ, hỗ trợ kỹ thuật, nội dung, thời gian báo cáo công tác đảm bảo an toàn, an ninh thông tin.

9. Tổng hợp báo cáo và thông báo về tình hình an toàn, an ninh thông tin mạng theo định kỳ cho UBND huyện, Sở Thông tin và Truyền thông và các cơ quan, đơn vị có liên quan.

10. Tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin

**Điều 14. Trách nhiệm của Công an xã**

1. Chủ trì, phối hợp với Văn phòng thống kê xã và các cơ quan, đơn vị có liên quan xây dựng kế hoạch và 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, an ninh thông tin mạng trong cơ quan nhà nước.

2. Phối hợp với các cơ quan chức năng trong trao đổi, kiểm tra, đảm bảo an toàn, an ninh thông tin.

3. Tăng cường công tác tuyên truyền, phổ biến pháp luật; tổ chức phòng ngừa, phát hiện, đấu tranh và xử lý nghiêm các hoạt động xâm hại đến an toàn, an ninh thông tin.

4. Điều tra và xử lý các trường hợp vi phạm pháp luật về lĩnh vực an toàn, an ninh thông tin mạng theo thẩm quyền.

5. Thực hiện nhiệm vụ bảo vệ an toàn các công trình quan trọng về an ninh quốc gia trên lĩnh vực công nghệ thông tin.

**Điều 15. Trách nhiệm của cán bộ, công chức, viên chức tại các cơ quan, đơn vị**

1. Trách nhiệm của cán bộ chuyên trách công nghệ thông tin:

a) Chịu trách nhiệm triển khai các biện pháp quản lý vận hành, quản lý kỹ thuật và tham mưu xây dựng các quy định về đảm bảo an toàn, an ninh thông tin mạng cho toàn bộ hệ thống thông tin của đơn vị mình đúng theo nội dung Quy định này.

b) Chủ động phối hợp với cá nhân, đơn vị có liên quan trong việc kiểm tra, phát hiện và khắc phục sự cố về an toàn, an ninh thông tin.

c) Tuân thủ theo sự hướng dẫn kỹ thuật của Văn phòng thống kê xã trong quá trình khắc phục sự cố về an toàn, an ninh thông tin.

2. Trách nhiệm của cán bộ, công chức, viên chức tham gia sử dụng và khai thác hệ thống thông tin:

a) Nghiêm túc thực hiện các nội quy, quy chế, quy trình nội bộ về đảm bảo an toàn, an ninh thông tin mạng của đơn vị cũng như các quy định khác của pháp luật về nội dung này.

b) Khi phát hiện nguy cơ hoặc sự cố mất an toàn, an ninh thông tin mạng phải báo cáo kịp thời cho cán bộ chuyên trách công nghệ thông tin của đơn vị mình để kịp thời ngăn chặn và xử lý.

c. Để đảm bảo bí mật nhà nước không bị lộ, lọt ra bên ngoài, gây thiệt hại nghiêm trọng thì từng cán bộ công chức, viên chức trong cơ quan phải làm bản cam kết (nếu cần).

d) Nâng cao ý thức cảnh giác và trách nhiệm về an toàn, an ninh thông tin.

**Điều 16. Trách nhiệm của các doanh nghiệp cung cấp hạ tầng mạng và dịch vụ Internet**

Các doanh nghiệp cung cấp hạ tầng mạng viễn thông và dịch vụ internet phải thiết lập đầu mối liên lạc để phối hợp và tuân thủ việc điều phối của cơ quan chức năng và tham gia vào công tác ứng cứu, khắc phục sự cố cho hệ thống thông tin quan trọng của tỉnh, của huyện.

Bảo đảm an toàn, bảo mật và tính riêng tư của thông tin, dữ liệu của cơ quan nhà nước; tuân thủ các quy định của pháp luật về an toàn, an ninh thông tin, cơ yếu và Pháp lệnh Bảo vệ bí mật nhà nước.

**Chương V**

**TỔ CHỨC THỰC HIỆN**

**Điều 19. Tổ chức thực hiện**

1. Văn hoá xã hội xã chủ trì, phối hợp với các cơ quan, đơn vị có liên quan triển khai thực hiện tốt nội dung Quy định này.

2. Các cơ quan, đơn vị chủ động xây dựng, ban hành Quy chế nội bộ về đảm bảo an toàn, an ninh thông tin mạng trong đơn vị minh phù hợp với Quy định này. Định kỳ hàng năm báo cáo tổng hợp tình hình đảm bảo an toàn, an ninh thông tin mạng tại đơn vị mình gửi Văn phòng thống kê xã để tổng hợp, báo cáo Ủy ban nhân dân huyện.

3. Thủ trưởng các cơ quan, đơn vị tổ chức triển khai thực hiện nghiêm túc Quy định này. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, phát sinh cần sửa đổi, bổ sung, đề nghị các cơ quan, đơn vị kịp thời báo cáo về Văn hoá xã hội xã xã để tổng hợp trình Ủy ban nhân dân xã xem xét, quyết định./.