|  |  |
| --- | --- |
| UBND THÀNH PHỐ KON TUM  **VĂN PHÒNG HĐND-UBND** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**  **Độc lập - Tự do - Hạnh phúc** |
| Số: /VP-TH  V/v đề nghị tham gia ý kiến đối với dự thảo Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan Nhà nước trên địa bàn Thành phố Kon Tum. | *TP. Kon Tum, ngày tháng 6 năm 2017* |

Kính gửi:

- Các đơn vị phòng, ban thành phố;

- Ủy ban nhân dân 21 xã, phường.

Nhằm đẩy mạnh hơn nữa công tác đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng CNTT tại các cơ quan, đơn vị trực thuộc thành phố.

Trên cơ sở hướng dẫn của Sở Thông tin và Truyền Thông tỉnh về việc xây dựng quy chế nội bộ về đảm bảo an toàn, an ninh thông tin,

Văn phòng HĐND-UBND thành phố đã xây dựng dự thảo Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan Nhà nước trên địa bàn thành phố *(dự thảo Quy chế được đăng tải trên trang thông tin điện tử của thành phố Kon Tum, mục Thông tin cần biết)*.

Văn phòng HĐND-UBND thành phố đề nghị các cơ quan, đơn vị tham gia ý kiến vào dự thảo trên.

Văn bản tham gia ý kiến của các cơ quan, đơn vị xin gửi về Văn phòng HĐND-UBND thành phố *(bản điện tử gửi qua địa chỉ email:* [*thaodang83kt@gmail.com*](mailto:thaodang83kt@gmail.com)*)*  **trước ngày 20/7/2017** để tổng hợp trình UBND thành phố ban hành. Nếu quá thời hạn trên, các đơn vị không tham gia ý kiến thì xem như thống nhất với các nội dung của dự thảo.

Văn phòng HĐND-UBND thành phố báo để các cơ quan, đơn vị biết, phối hợp thực hiện./.

|  |  |
| --- | --- |
| ***Nơi nhận:***  - Như trên (p/h);  - Đ/c Ninh – PCT UBND (b/c);  - Lãnh đạo VP;  - Lưu: VT, VP. | **CHÁNH VĂN PHÒNG**  **Nguyễn Quốc Vương** |

**ỦY BAN NHÂN DÂN CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**

**THÀNH PHỐ KON TUM Độc lập - Tự do - Hạnh phúc**

Số: /QĐ-UBND *TP. Kon Tum, ngày tháng 7 năm 2017*

**QUYẾT ĐỊNH**

###### V/v Ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động

###### ứng dụng công nghệ thông tin của các cơ quan nhà nước

###### trên địa bàn Thành phố Kon Tum

**ỦY BAN NHÂN DÂN THÀNH PHỐ KON TUM**

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19 tháng 6 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 72/2013/NĐ-CP ngày 15 tháng 7 năm 2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng;

Căn cứ Quyết định số 898/QĐ-TTg ngày 27 tháng 5 năm 2016 của Thủ tướng Chính phủ phê duyệt phương hướng nhiệm vụ bảo đảm an toàn thông tin mạng giai đoạn 2016-2020;

Căn cứ Quyết định số 24/2016/QĐ-UBND ngày 17 tháng 6 năm 2016 của Ủy ban nhân dân tỉnh kon Tum về việc Ban hành quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Kon Tum;

Xét đề nghị của Chánh Văn phòng HĐND và UBND thành phố Kon Tum tại Tờ trình số /TTr-VP ngày tháng 7 năm 2017,

# QUYẾT ĐỊNH:

**Điều 1.** Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn thành phố Kon Tum.

**Điều 2.** Chánh Văn phòng HĐND và UBND, Thủ trưởng các đơn vị phòng, ban thành phố; Chủ tịch Ủy ban nhân dân các xã, phường và các cơ quan, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này.

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

***Nơi nhận:***   **TM. ỦY BAN NHÂN DÂN**

- Sở Thông tin & Truyền thông tỉnh; **CHỦ TỊCH**

- TT. Thành ủy;

- TT. HĐND thành phố;

- Lãnh đạo UBND thành phố;

- Các đơn vị phòng, ban thành phố;

- UBND 21 xã, phường;

- Như Điều 2;

- Lưu: VT, UB.

|  |  |
| --- | --- |
| **ỦY BAN NHÂN DÂN**  **THÀNH PHỐ KON TUM** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**  **Độc lập – Tự do – Hạnh phúc** |

**DỰ THẢO**

**QUY CHẾ**

**Về đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng**

**công nghệ thông tin của các cơ quan Nhà nước**

**trên địa bàn Thành phố Kon Tum**

**Chương I**

**QUY ĐỊNH CHUNG**

**Điều 1. Phạm vi điều chỉnh**

**1.** Quy chế này quy định về công tác đảm bảo an toàn, an ninh thông tin (AT-ANTT) trong hoạt động ứng dụng công nghệ thông tin (CNTT) của các cơ quan hành chính Nhà nước trên địa bàn thành phố Kon Tum.

**2.** Đối với lực lượng vũ trang ngoài việc thực hiện các quy định tại Quy chế này, các quy định khác của pháp luật có liên quan còn phải thực hiện theo quy định của ngành trong đảm bảo an ninh thông tin, bảo mật trên môi trường mạng.

**Điều 2. Đối tượng áp dụng**

**1.** Quy chế này áp dụng đối với các cơ quan, đơn vị trên địa bàn thành phố Kon Tum, bao gồm:

**a)** Ủy ban nhân dân thành phố và các cơ quan chuyên môn trực thuộc;

**b)** Ủy ban nhân dân các xã, phường;

**c)** Các đơn vị sự nghiệp thuộc cơ quan quản lý nhà nước (QLNN) của UBND thành phố

**đ)** Các tổ chức, cá nhân có liên quan khi tham gia sử dụng hệ thống thông tin của cơ quan nhà nước, để giao tiếp, cung cấp và trao đổi thông tin số với cơ quan nhà nước.

**2.** Cán bộ, công chức, viên chức và người lao động đang làm việc tại các đơn vị quy định tại “Khoản 1 Điều này”.

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

**1.** Việc áp dụng Quy chế này nhằm giảm thiểu các nguy cơ gây mất an toàn thông tin và đảm bảo an ninh thông tin trong quá trình ứng dụng CNTT trong hoạt động của các cơ quan.

**2.** Các hoạt động ứng dụng CNTT phải tuân theo nguyên tắc đảm bảo an toàn thông tin được quy định tại Điều 41, Nghị định 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng CNTT trong hoạt động của cơ quan nhà nước.

**Đỉều 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 địch vụ CNTT.

**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 đựng 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.** Log File: là một tập tin được tạo ra bởi một máy chủ có chứa tất cả thông tin về các hoạt động trên máy chủ đó.

**8.** Firewall (tường lửa): là rào chắn (phần cứng, phần mềm) được lập ra nhằm kiểm soát người dùng mạng Internet truy nhập vào các thông tin không mong muốn và người dùng từ bên ngoài truy nhập trái phép thông tin trong mạng nội bộ.

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

**Chương II**

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

**Điều 5. Điều kiện đảm bảo thực hiện nhiệm vụ an toàn, an ninh thông tin**

**1.** Cán bộ, công chức, viên chức, người sử dụng hệ thống thông tin phải nắm vững các kiến thức cơ bản, quy định pháp luật và nội quy của cơ quan, đơn vị về an toàn, an ninh thông tin.

**2.** Các cơ quan, đơn vị, tổ chức bố trí cán bộ chuyên trách hoặc kiêm nhiệm phụ trách CNTT của cơ quan, đơn vị mình.

**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.** Duy trì và đảm bảo công tác theo dõi, kiểm tra, thống kê, tổng hợp, báo cáo định kỳ và đột xuất; Có hình thức khen thưởng hoặc xử lý kịp thời theo quy định.

**Điều 6. Quản lý trang thiết bị và hạ tầng công nghệ thông tin**

**1. Đối với máy chủ:**

**a)** Phòng máy chủ của cơ quan, đơn vị phải độc lập, do bộ phận chuyên trách CNTT trực tiếp quản lý, các cán bộ không liên quan không được vào phòng máy chủ. Phòng máy chủ phải đảm bảo khô, thoáng, nguồn điện cung cấp đảm bảo tính ổn định cao. Phòng máy chủ phải được trang bị máy lạnh và vận hành liên tục. Tùy theo điều kiện của từng đơn vị trực thuộc mà bố trí phòng máy chủ riêng hoặc có thể ghép chung với bộ phận khác nhưng vẫn đảm bảo máy chủ hoạt động ổn định và vận hành liên tục.

**b)** Cấu hình máy chủ phải đủ mạnh để đáp ứng công việc. Máy chủ của các cơ quan chỉ dùng để triển khai phần mềm hệ thống, cài đặt phần mềm dùng chung, các phần mềm chống virus, các cơ sở dữ liệu cần thiết và các phần mềm mềm có bản quyền hỗ trợ cho việc triển khai hệ thống thông tin, ngoài ra không được cài đặt các phần mềm không rõ nguồn gốc phần mềm không có nhu cầu sử dụng.

**c)** Không sử dụng máy chủ cho việc duyệt web đọc báo, xem tin tức,...

**đ)** Cài đặt phần mềm diệt virus có bản quyền cho tất cả các máy chủ.

**e)** Thiết lập chế độ tự động cập nhật bảnvá lỗ hổng bảo mật cho phần mềm hệ điều hành và các phần mềm ứng dụng được cài đặt trên máy chủ; đóng tất cả các cổng (Port) dịch vụ khi không sử dụng; thiết lập chính sách ghi lưu tập trung quá trình hoạt động (Log file) của mỗi máy chủ theo định kỳ từ 03 tháng trở lên.

**f)** Khi cần kết nối từ xa, nhất là từ Internet vào máy chủ để sử dụng hoặc quản trị, đề nghị sử dụng một trong các phương thức kết nối có mã hóa như: SSH, VPN, FTPs,... để đảm bảo an toàn thông tin.

**2.** Thiết bị chống sét, phòng cháy, chữa cháy: Lắp đặt và thường xuyên bảo trì các thiết bị chống sét, trang bị thiết bị phòng cháy, chữa cháy để bảo vệ hệ thống thông tin của cơ quan, đơn vị.

**3.** CBCCVC có trách nhiệm quản lý trang thiết bị CNTT (máy vi tính, máy in, thiết bị ngoại vi,…) được giao sử dụng, tự quản lý dữ liệu trên máy tính của cá nhân, tự quyết định việc chia sẻ tài nguyên với các máy tính khác theo đúng quy định.

**4.** Cán bộ phụ trách CNTT của thành phố và các cán bộ kiêm nhiệm CNTT của các cơ quan, đơn vị chịu trách nhiệm kiểm tra, theo dõi, đánh giá sự hoạt động của máy chủ, máy trạm, các thiết bị mạng và các thiết bị ngoại vi theo đúng tiêu chuẩn kỹ thuật; thực hiện việc sao lưu dữ liệu thường xuyên; các thiết bị CNTT phải thực hiện công tác bảo trì, bảo dưỡng định kỳ, đột xuất, giảm thiểu tối đa các sự cố kỹ thuật.

**5.** Máy vi tính chứa dữ liệu quan trọng và thường xuyên kết nối Internet phải cài đặt các phần mềm diệt virus có bản quyền; có cơ chế bảo vệ thư mục và tập tin khi chia sẻ tài nguyên dùng chung.

**6.** Máy tính và các thiết bị CNTT để nơi an toàn, tránh ảnh hưởng của các tác nhân bên ngoài như nắng, mưa…; không để các tài liệu, vật liệu dễ cháy gần máy tính và các thiết bị CNTT để tránh xảy ra cháy nổ; thường xuyên vệ sinh cho máy vi tính; hàng ngày kiểm tra theo dõi sự hoạt động của máy vi tính và các thiết bị... Khi không sử dụng nên tắt máy vi tính và các thiết bị nhằm tiết kiệm điện và phòng, chống cháy nổ và các hành vi xâm nhập trái phép.

**7.** Trong quá trình sử dụng các thiết bị CNTT, khi có sự cố xảy ra đối với các thiết bị CNTT của CBCCVC, người sử dụng thiết bị CNTT thông báo với cán bộ phụ trách CNTT của cơ quan, đơn vị; nếu sự cố nhỏ, không phải thay thế hoặc sửa chữa linh kiện thì cán bộ được giao phụ trách CNTT của cơ quan, đơn vị xử lý trực tiếp. Nếu có sự cố lớn, cần phải thay thế linh kiện để sửa chữa thì người dùng thiết bị CNTT phải làm đề xuất, có xác nhận của lãnh đạo cơ quan, đơn vị; khi thanh lý tài sản là thiết bị công nghệ thông tin như máy trạm, máy chủ,... không được thanh lý ổ cứng và các thiết bị lưu trữ dữ liệu mà phải tiêu hủy theo quy định.

**8.** 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 AT-ANTT mạng.

**9.** **Đối với hệ thống mạng LAN:**

**a)** CBCCVC của cơ quan, đơn vị khi tham gia vào mạng LAN không được tự ý thay đổi các tham số và đấu nối các thiết bị mạng, nếu tự ý thay đổi tham số, thiết bị mạng thì người thay đổi phải chịu hoàn toàn trách nhiệm. Trường hợp cần thiết phải thay đổi tham số, thiết bị mạng, phải báo cán bộ phụ trách CNTT của cơ quan, đơn vị biết để theo dõi, xử lý.

**b)** Cán bộ phụ trách CNTT chịu trách nhiệm cung cấp địa chỉ IP mạng và tham số mạng cho người dùng kết nối vào mạng LAN của cơ quan; hướng dẫn, cài đặt hệ thống an ninh mạng theo đúng tiêu chuẩn an toàn bảo mật; xử lý khắc phục kịp thời khi xảy ra sự cố, đảm bảo hệ thống mạng máy tính hoạt động ổn định, liên tục.

**10.** Hàng năm cán bộ phụ trách CNTT đề xuất kế hoạch mua sắm các thiết bị CNTT để đảm bảo an toàn cho các máy tính và mạng máy tính của cơ quan, đơn vị mình.

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

**1.** Quản lý tài nguyên: Cán bộ quản trị mạng có trách nhiệm kiểm tra, giám sát chức năng chia sẻ thông tin; 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 cá nhân 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 06 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 (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 hưởng đến hoạt động của hệ thống.

**5.** Phòng chống mã độc, virus: Trên các máy chủ và 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 các 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 phụ 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 đùng chung đảm bảo tránh được các xung đột và gây mất an toàn thông tin.

**Điều 8. Sử dụng an toàn Hệ điều hành**

**1.** Thay thế Windows XP bằng hệ điều hành mới được hỗ trợ tốt hơn *(Windows7, Windows8, Windows10…)*, trong đó ưu tiên sử dụng các hệ điều hành mã nguồn mở (Linux). Trường hợp chưa có điều kiện cài đặt hệ điều hành mới thay thế Windows XP cần thực hiện các biện pháp sau:

**a)** Sử dụng tường lửa được tích hợp sẵn trên hệ điều hành, kết hợp với tường lửa của hệ thống mạng để quản lý các truy cập.

**b)** Gõ bỏ hoặc tắt các dịch vụ không dùng đến hoặc ít dùng như: Netmeeting, Remote Desktop Sharing, Remote Desktop, Remote Registry, Routing & Remote Access, SSDP Discovery Service, Universal Plug and Play Device Host, Telnet, SMB vv...

**c)** Sử đụng các trình duyệt web như Firefox, Mozilla, Chrome để thay thế cho trình duyệt Internet Explorer đi kèm theo Windows XP.

**d)** Không tải (download) và cài đặt các bản vá lỗi mà không rõ nguồn gốc, kiểm tra tính toàn vẹn các bản vá lỗi trước khi sử dụng.

**e)** Tạo các bản sao dữ liệu, hệ thống để hỗ trợ việc phục hồi hệ thống.

**f)** Đặt mật khẩu đăng nhập cho máy tính cá nhân nhằm hạn chế các nguy cơ xâm nhập trái phép.

**g)** Tắt bỏ tính năng tự động chạy ứng dụng (Autorun) khi kết nối với thiết bị lưu trữ ngoài (như thẻ nhớ ngoài giao tiếp qua cổng USB) để giảm nguy cơ lây lan mã độc thông qua việc sao chép thông tin.

**h)** Tắt máy tính, đăng xuất khỏi hệ thống hoặc khóa màn hình (có mật khẩu) khi không sử dụng trong thời gian đài (quá 02 giờ làm việc).

**Điều 9. 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; không cung cấp tin, tài liệu và đưa thông tin bí mật nhà nước trên Trang thông tin điện tử, hộp thư điện tử và các dịch vụ lưu trữ trực tuyến (Dropbox, Google Drive, Microsoft OneDriver, iCloud…)

**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 phụ trách CNTT phải dùng các biện pháp kỹ thuật xoá bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

**Điều 10. 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 trên các thiết bị lưu trữ dữ liệu.

**2.** Thiết bị lưu trữ dữ liệu 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.

**3.** 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 và điều kiện thực tế của đơn vị.

**4.** 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 AT-ANTT; chức năng không cho người dùng truy cập một số website không phù hợp với quy định hiện hành.

**5.** Hệ thống mạng không dây (wireless) của các cơ quan, đơn vị phải được thiết lập mật khẩu khi truy cập tối thiểu 06 ký tự.

**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 06 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 thiêt lập phù hợp cho từng đối tượng.

**Điều 11. Quyền hạn, nhiệm vụ của cán bộ phụ trách CNTT của cơ quan, 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 AT-ANTT.

**2.** Quản lý chặt chẽ việc di chuyển các trang thiết bị CNTT 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 đảm bảo AT-ANTT 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 AT-ANTT 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.

**Chương III**

**TRÁCH NHIỆM ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN MẠNG**

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

**1.** Người đứng đầu các cơ quan, đơn vị, địa phương chịu trách nhiệm trong công tác đảm bảo AT-ANTT đối với toàn bộ hệ thống thông tin mạng của cơ quan, đơn vị, địa phương mình.

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

**3.** Tạo điều kiện thuận lợi cho cán bộ phụ trách về CNTT được đào tạo, bồi dưỡng chuyên môn trong lĩnh vực AT-ANTT mạng.

**4.** Quan tâm đầu tư các thiết bị phần cứng, phần mềm liên quan đến công tác đảm bảo AT-ANTT.

**5.** Khi có sự cố hoặc nguy cơ mất AT-ANTT 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 cấp trên.

**Điều 13. Trách nhiệm của Phòng Văn hóa – Thông tin thành phố**

**1.** Chịu trách nhiệm trước Ủy ban nhân dân thành phố về công tác đảm bảo AT-ANTT trong hoạt động ứng dụng CNTT của các cơ quan nhà nước trên phạm vi toàn thành phố.

**2.** Chủ trì, phối hợp với Văn phòng HĐND-UBND thành phố và các đơn vị liên quan tham mưu Ủy ban nhân dân thành phố ban hành các văn bản chỉ đạo, kế hoạch nhằm đảm bảo AT-ANTT.

**3.** Phối hợp với Phòng Tài chính – Kế hoạch thành phố, Văn phòng HĐND-UBND thành phố xây dựng kế hoạch, tổng hợp kinh phí để triển khai công tác AT-ANTT trong hoạt động ứng dụng CNTT của UBND thành phố.

**4.** Phối hợp với các cơ quan liên quan trong công tác kiểm tra định kỳ hoặc đột xuất khi phát hiện có các dấu hiệu, hành vi vi phạm AT-ANTT.

**5.** Tham mưu cho Ủy ban nhân dân thành phố thành phố triển khai các chương trình đào tạo, bồi dưỡng, hội nghị AT-ANTT trên địa bàn thành phố.

**6.** Thông báo cho các cơ quan, đơn vị biết để có biện pháp phòng ngừa, ngăn chặn các nguy cơ mất AT-ANTT do virus, phần mềm gián điệp,... gây ra.

**7.** Phối hợp với Công an thành phố và các đơn vị liên quan trong điều tra làm rõ các nguyên nhân gây ra sự cố mất AT-ANTT.

**Điều 14. Trách nhiệm của phòng Văn phòng HĐND-UBND thành phố**

**1.** Trực tiếp quản lý vận hành và chịu trách nhiệm về công tác đảm bảo AT-ANTT đối với các hệ thống thông tin của Ủy ban nhân dân thành phố.

**2.** Phối hợp với phòng Văn hóa – Thông tin thành phố và các đơn vị có liên quan đảm bảo AT-ANTT trong hoạt động ứng dụng CNTT trên địa bàn thành phố.

**Điều 15. Trách nhiệm của Công an thành phố**

**1.** Chủ trì, phối hợp với Phòng Văn hóa - Thông tin thành phố, Văn phòng HĐND-UBND thành phố, và các cơ quan liên quan thực hiện quản lý, kiểm soát, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống thông tin xâm hại đến an ninh chính trị, trật tự an toàn xã hội.

**2.** Định kỳ thông báo cho các cơ quan về phương thức, thủ đoạn mới của các loại tội phạm xâm hại đến AT-ANTT để có biện pháp phòng ngừa, đấu tranh.

**3.** Điều tra làm rõ các trường hợp vi phạm AT-ANTT và xử lý đúng quy định của pháp luật.

**4.** Phối hợp với các cơ quan, đơn vị cấp tỉnh trong việc triển khai thực hiện kế hoạch bảo vệ an toàn các công trình quan trọng về an ninh quốc gia trên lĩnh vực CNTT trên địa bàn thành phố.

**Điều 16. Trách nhiệm của cán bộ, công chức, viên chức và người lao động tại các cơ quan, đơn vị**

**1. Trách nhiệm của cán bộ phụ 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 AT-ANTT mạng cho toàn bộ hệ thống thông tin của đơn vị mình đúng theo nội dung Quy chế 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 AT-ANTT.

**c)** 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.

**d)** Lập biên bản ghi nhận sự cố gây ra mất AT-ANTT 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.

**e)** 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.

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

**a)** Nghiêm túc chấp hành các quy định, quy trình nội bộ, Quy chế này và các quy định khác của pháp luật về AT-ANTT. Chịu trách nhiệm đảm bảo AT-ANTT trong phạm vi trách nhiệm và quyền hạn được giao.

**b)** Quản lý chặt chẽ việc di chuyển các trang thiết bị CNTT lưu trữ các thông tin thuộc đanh mục bí mật nhà nước.

**c)** Khi phát hiện nguy cơ hoặc sự cố mất an toàn, an ninh thông tin mạng phải báo cáo kịp thời cho cán bộ phụ trách CNTT của đơn vị mình để kịp thời ngăn chặn và xử lý. Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

**Chương IV**

**TỔ CHỨC THỰC HIỆN**

**Điều 17. Cán bộ phụ trách CNTT thành phố**

**1.** Trực tiếp tham mưu xử lý, khắc phục sự cố, hướng dẫn khắc phục sự cố về AT-ANTT của thành phố.

**2.** Thường xuyên hướng dẫn CBCCVC khai thác và sử dụng tài nguyên CNTT và đảm bảo AT-ANTT.

**Điều 18. Phòng Văn hóa và Thông tin thành phố**

**1.** Chủ trì phối hợp với các cơ quan liên quan đôn đốc, hướng dẫn việc thực hiện nghiêm túc Quy chế này và báo cáo Ủy ban nhân dân thành phố về AT-ANTT theo quy định.

**2.** Phối hợp với Văn phòng HĐND-UBND tổng hợp các vướng mắc, đề nghị bổ sung, chỉnh sửa quy chế; tham mưu đề xuất đầu tư kinh phí mua các phần mềm, thiết bị và hạ tầng kỹ thuật để đảm bảo AT-ANTT cho thành phố.

**Điều 19. Phòng Tài chính – Kế hoạch thành phố**

Phối hợp với Phòng Văn hóa – Thông tin thành phố và Văn phòng HĐND-UBND thành phố tham mưu Ủy ban nhân dân thành phố xem xét ưu tiên bố trí kinh phí thực hiện các nhiệm vụ đảm bảo AT-ANTT của thành phố.

**Điều 20. Phòng Nội vụ thành phố**

Đưa mức độ về đảm bảo AT-ANTT trở thành một trong các tiêu chí bình xét thi đua, khen thưởng hàng năm của các cơ quan, đơn vị.

**Điều 21. Khen thưởng và xử lý vi phạm**

**1.** Hằng năm, Phòng Văn hóa – Thông tin chủ trì phối hợp với Văn phòng HDDND-UBND thành phố dựa trên các điều tra, báo cáo công tác AT-ANTT của các cơ quan, đơn vị để xác lập bảng đánh giá xếp hạng AT-ANTT, trên cơ sở đó đề xuất Ủy ban nhân dân thành phố xem xét khen thưởng theo quy định hiện hành.

**2.** Các cơ quan, đơn vị và CBCCVC trong các cơ quan, đơn vị trên địa bàn thành phố vi phạm quy định này thì tùy theo tính chất, mức độ vi phạm sẽ bị xử lý kỷ luật theo trách nhiệm, xử phạt hành chính, bồi thường thiệt hại hoặc truy cứu trách nhiệm hình sự theo quy định hiện hành.

**Điều 22. Điều khoản thi hành**

**1.** Thủ trưởng cơ quan, đơn vị trực thuộc thành phố, Chủ tịch Ủy ban nhân dân các xã, phường và các đơn vị có liên quan chịu trách nhiệm tổ chức triển khai thực hiện Quy chế này.

**2.** Trong quá trình thực hiện nếu có vấn đề phát sinh, vướng mắc, CBCCVC các cơ quan, đơn vị, UBND các xã, phường phản ánh kịp thời về Phòng Văn hóa và Thông tin thành phố để tổng hợp trình UBND thành phố xem xét, quyết định./.

**TM. ỦY BAN NHÂN DÂN**

**CHỦ TỊCH**

**Phụ lục I**

**MẪU BÁO CÁO ĐỊNH KỲ VỀ AN TOÀN THÔNG TIN**

*(Ban hành kèm theo Quyết định số /QĐ-UBND ngày tháng 7 năm 2017  
của Ủy ban nhân dân thành phố Kon Tum)*

|  |  |
| --- | --- |
| Tên Cơ quan/Đơn vị:…….  …………………………..  Số: ……. | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**  **Độc lập - Tự do - Hạnh phúc**  *TP. Kon Tum, ngày tháng năm 20* |

**BÁO CÁO ĐỊNH KỲ VỀ AN TOÀN THÔNG TIN**

Kính gửi: Ủy ban nhân dân thành phố Kon Tum.

**I. Tình hình an toàn thông tin tại cơ quan/đơn vị:**

1. Ban hành Quy chế an toàn thông tin tại cơ quan/đơn vị: 🞏 Có 🞏 Không

Nếu có: (ghi rõ số Quyết định và ngày ban hành) ……………………………………

2. Tổng số máy tính của cơ quan/đơn vị, trong đó: …. máy chủ; ….. máy trạm

3. Cơ quan/đơn vị có kết nối mạng cục bộ (LAN): 🞏 Có 🞏 Không

Nếu có, mạng LAN được thiết kế theo mô hình:

🞏 Client/Server có đăng nhập Domain 🞏 ngang hàng (Peer to Peer)

4. Cơ quan/đơn vị tự trang bị đường truyền kết nối Internet: 🞏 Có 🞏 Không

Nếu có: ghi rõ tên nhà cung cấp dịch vụ đường truyền Internet: ……………………

Số máy tính kết nối mạng Internet: ………...máy, trong đó:

Số máy tính không kết nối mạng internet để soạn thảo các văn bản mật:……….. máy.

5. Đơn vị có đầu tư thiết bị, giải pháp đảm bảo an toàn thông tin:

- Thiết bị tường lửa (Firewall): 🞏 Có 🞏 Không

Nếu có: (ghi cụ thể tên, số hiệu, tường lửa là thiết bị phần cứng, hay phần mềm)…….

- Phần mềm diệt virus: 🞏 Có 🞏 Không

Nếu có, tổng số máy tính có cài phần mềm diệt vius có bản quyền………… máy, trong đó: …. máy chủ, ….. máy trạm.

- Giải pháp khác (ghi cụ thể):………………………………..…………..……………

6. Chi phí đầu tư cho an toàn thông tin trong thời gian qua (kỳ báo cáo):……………

7. Dự kiến Chi phí đầu tư cho an toàn thông tin trong thời gian tới:…………………

8. Cơ quan/đơn vị có hệ thống thư điện tử riêng (ngoài hệ thống thư điện tử chung của thành phố @cantho.gov.vn): 🞏 Có 🞏 Không

Nếu có (ghi cụ thể):…………………………………………….

9. Cơ quan/đơn vị sử dụng hòm thư công cộng, công nghệ lưu trữ điện toán đám mây công cộng (ví dụ: Gmail, Yahoo Mail, Google Drive, One Drive, ….) để lưu trữ, trao đổi tài liệu quan trọng của cơ quan/đơn vị: 🞏 Có 🞏 Không

Cơ quan/đơn vị có nhu cầu sử dụng công nghệ lưu trữ điện toán đám mây dùng riêng tại Trung tâm Dữ liệu thành phố: 🞏 Có 🞏 Không

10. Cơ quan/đơn vị có lắp đặt và sử dụng mạng không dây (wifi): 🞏 Có 🞏 Không

Nếu có:

+ Người quản trị có đổi lại mật khẩu quản trị mặc định của Access Point/Router ADSL: 🞏 Có 🞏 Không

+ Đặt mật khẩu wifi để truy cập: 🞏 Có 🞏 Không

+ Đặt địa chỉ MAC cho các thiết bị di động (chỉ dành riêng cho người dùng nội bộ của đơn vị): 🞏 Có 🞏 Không

+ Phân chia vùng cho người dùng thuộc cơ quan/đơn vị hay người dùng công cộng: 🞏 Có 🞏 Không

11. Thống kê sự cố về an toàn thông tin (trong kỳ báo cáo)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Loại sự cố** | **Tổng**  **số lượng** | **Số sự cố tự xử lý** | **Số sự cố đề nghị Sở Thông tin và Truyền thông hỗ trợ xử lý** | **Số sự cố có sự hỗ trợ xử lý từ các tổ chức khác (bao gồm tổ chức trong và ngoài nước)** | **Thiệt hại ước tính (VNĐ)** |
| Tấn công từ chối dịch vụ (Dos, Ddos) |  |  |  |  |  |
| Mã độc (Spyware/Adware) |  |  |  |  |  |
| Thay đổi giao diện website |  |  |  |  |  |
| Lừa đảo (Phishing) |  |  |  |  |  |
| Virus |  |  |  |  |  |
| Khác:…………………….. |  |  |  |  |  |

**II. Nhân lực về an toàn thông tin**

1. Cơ quan/đơn vị có phân công lãnh đạo phụ trách về an toàn thông tin:

🞏 Có 🞏 Không

2. Cơ quan/đơn vị có phân công bộ phận/cán bộ phụ trách về an toàn thông tin:

🞏 Có 🞏 Không

Nếu có (ghi rõ họ tên, email, điện thoại liên hệ):……………………………………..

3. Hiện trạng cán bộ, công chức, viên chức được đào tạo về an toàn thông tin:

+ Cán bộ cán bộ lãnh đạo, quản lý (từ cấp lãnh đạo phòng, ban trở lên), số lượng: ………….. người

+ Cán bộ chuyên trách an toàn thông tin, số lượng: ………….. người

+ Cán bộ, công chức, viên chức khác (người dùng), số lượng: ………….. người

4. Nhu cầu đào tạo nhân lực về an toàn thông tin:

+ Dành cho cán bộ lãnh đạo, quản lý (từ cấp lãnh đạo phòng, ban trở lên), số lượng dự kiến: ………….. người

+ Dành cho cán bộ chuyên trách an toàn thông tin, số lượng dự kiến: ……….. người

+ Dành cho người cán bộ, công chức, viên chức (người dùng), số lượng dự kiến: ………….. người

**III. Ý kiến phản hồi, đề xuất, kiến nghị:**

……………………………………………………………………………..…….......

……………………………………………………………………………..…….......

……………………………………………………………………………..…….......

**Người lập báo cáo Thủ trưởng Cơ quan/Đơn vị**

*(Ký, ghi rõ họ tên) (Ký, ghi rõ họ tên, đóng dấu)*

**Phụ lục II**

**MẪU THÔNG BÁO SỰ CỐ AN TOÀN THÔNG TIN**

*(Ban hành kèm theo Quyết định số /QĐ-UBND ngày tháng 7 năm 2017*

*của Ủy ban nhân dân thành phố Kon Tum)*

|  |  |
| --- | --- |
| Tên Cơ quan/Đơn vị:………  ......................................................  Số: ……. | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**  **Độc lập - Tự do - Hạnh phúc**  *Tp. Kon Tum, ngày tháng năm 20* |

Kính gửi: Ủy ban nhân dân thành phố Kon Tum.

**1. Thông tin về sự cố**

* Mô tả sơ bộ về sự cố:

* Cách thức phát hiện (*Đánh dấu những cách thức được sử dụng để phát hiện sự cố)*

🞏 Qua hệ thống phát hiện xâm nhập (IDS ) 🞏 Kiểm tra Log File 🞏 Quản trị hệ thống 🞏 Khác:

* Thời gian xảy ra sự cố : …/… /……/…/… (ngày/tháng/năm/giờ/phút)
* Thời gian thực hiện báo cáo sự cố: …/… /……/…/… (ngày/tháng/năm/giờ/phút)
* Người liên hệ (Họ tên, địa chỉ email, số điện thoại):

**2. Thông tin về hệ thống xảy ra sự cố**

* Hệ điều hành: version:
* Các dịch vụ có trên hệ thống (*Đánh dấu những dịch vụ được sử dụng trên hệ thống)*

🞏 Web server 🞏 Mail server 🞏 Database server

🞏 FTP server 🞏 Proxy server 🞏 Application server

🞏 Dịch vụ khác:

* Các địa chỉ IP của hệ thống:

* Các tên miền của hệ thống:

* Mục đích chính sử dụng hệ thống:

**Người lập Thủ trưởng Cơ quan/Đơn vị**

*(Ký, ghi rõ họ tên) (Ký, ghi rõ họ tên, đóng dấu)*