UBND TỈNH HÀ NAM **SỞ THÔNG TIN VÀ TRUYỀN THÔNG**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 51 /STTTT-CNTT	*Hà Nam, ngày 23 tháng 6 năm 2017*
V/v thẩm định dự thảo Quy chế đảm bảo ATTT trên máy tính, mạng máy tính và các thiết bị công nghệ thông tin trong hoạt động của các cơ quan nhà nước	

Kính gửi: Sở Tư pháp tỉnh Hà Nam

Thực hiện Quyết định số 79/QĐ-UBND ngày 16 tháng 01 năm 2017 của Uỷ ban nhân dân tỉnh về việc ban hành Chương trình công tác năm 2017, trong đó giao nhiệm vụ cho Sở Thông tin và Truyền thông dự thảo Qúy chế đảm bảo an toàn thông tin trên máy tính, mạng máy tính và các thiết bị công nghệ thông tin trong hoạt động của các cơ quan nhà nước tỉnh Hà Nam, Sở Thông tin và Truyền thông đã thực hiện các bước sau:

Bước 1: Cử nhóm cán bộ, chuyên viên soạn thảo và tổ chức Hội thảo nội bộ đóng góp ý kiến cho dự thảo Quy chế đảm bảo an toàn thông tin trên máy tính, mạng máy tính và các thiết bị công nghệ thông tin trong hoạt động của các cơ quan nhà nước tỉnh Hà Nam.

Bước 2: Gửi dự thảo Quy chế đến các sở, ban, ngành, ủy ban nhân dân huyện, thành phố để xin ý kiến đóng góp, bổ sung.

Bước 3: Tổng hợp ý kiến đóng góp của các cơ quan và chỉnh sửa dự thảo.

(Kèm theo công văn là dự thảo Quy chế; bản giải trình, tiếp thu ý kiến đóng góp của các sở, ban, ngành, UBND huyện, thành phố).

Đề nghị Sở Tư pháp thẩm định, cho ý kiến để Sở Thông tin và Truyền thông trình Ủy ban nhân dân tỉnh ban hành Quy chế./.

Nơi nhận: - Như trên; - Lưu VT.	**KT.GIÁM ĐỐC** **PHÓ GIÁM ĐỐC** CỘNG HÒA XHCN VIỆT NAM SỞ THÔNG TIN VÀ TRUYỀN THÔNG TỈNH HÀ NAM **Nguyễn Đức Cường**

Tổng hợp giải trình và tiếp thu ý kiến đóng góp của các cơ quan

(Kèm theo Tờ trình số: 51/TTr-STTTT ngày 23 tháng 6 năm 2017 của Sở Thông tin và Truyền thông)

STT	Tên đơn vị	Nội dung góp ý	Giải trình
1	Sở Tư pháp	- Đề nghị cơ quan soạn thảo bổ sung dự thảo Quyết định ban hành Quy chế.	Đã tiếp thu và chỉnh sửa
		- Tại khoản 2 Điều 1 dự thảo, đề nghị sửa: "UBND huyện, thành phố" thành "UBND các huyện, thành phố"	Không tiếp thu vì không có ủy ban nhân dân các huyện, thành phố.
		- Tại điểm b khoản 1 Điều 3 dự thảo Quy chế, đề nghị bổ sung: "Tuân thủ quy định của Luật An toàn thông tin mạng và các quy định khác của pháp luật có liên quan".	Đã tiếp thu và chỉnh sửa
		- Tên chương II dự thảo, đề nghị sửa thành: "Quy định đảm bảo an toàn thông tin mạng", tên Chương III dự thảo, đề nghị sửa thành: "Trách nhiệm đảm bảo an toàn thông tin mạng"	Không tiếp thu vì đây là quy chế đảm bảo an toàn thông tin cho cả các thiết bị không kết nối mạng.
2	Sở Xây dựng	- Tại Khoản 2, Điều 1. Quy chế này áp dụng đối với: Đề nghị bỏ gạch đầu dòng thứ 3 và chỉnh sửa gạch đầu dòng thứ 2: "Các tổ chức, cá nhân có tham gia quản lý, vận hành, khai thác và sử dụng… của tỉnh". Vì, cá nhân được hiểu bao gồm cả cán bộ, công chức, viên chức, người lao động…	Đã tiếp thu và chỉnh sửa
		- Việc đảm bảo ATTT trên máy tính, mạng máy tính và các thiết bị công nghệ thông tin trong hoạt động của các cơ quan nhà nước đồng thời với việc bố trí kinh phí kịp thời để nâng cấp hệ thống hạ tầng công nghệ thông tin và hệ thống máy tính, đảm bảo kết nối đồng bộ, thông suốt trong quá trình khai thác sử dụng (thực tế hiện nay chưa thể đáp ứng được quy định này).	Không tiếp thu vì trước mắt có thể chưa được đầu tư đồng bộ nhưng trong những năm tiếp theo sẽ đầu tư.

ỦY BAN NHÂN DÂN TỈNH HÀ NAM	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: /2017/QĐ-UBND	*Hà Nam, ngày tháng năm 2017*

QUYẾT ĐỊNH

Ban hành Quy chế Đảm bảo an toàn thông tin trên máy tính, mạng máy tính và các thiết bị công nghệ thông tin trong hoạt động của các cơ quan nhà nước tỉnh Hà Nam

ỦY BAN NHÂN DÂN TỈNH HÀ NAM

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

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 Pháp lệnh bảo vệ bí mật nhà nước số 30/2000/PL-UBTVQH10 ngày 28 tháng 12 năm 2000 của Ủy ban Thường vụ Quốc hội;

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 cơ quan nhà nước.

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế Đảm bảo an toàn thông tin trên máy tính, mạng máy tính và các thiết bị công nghệ thông tin trong hoạt động của các cơ quan nhà nước tỉnh Hà Nam.

Điều 2. Quyết định này có hiệu lực thi hành từ ngày tháng 7 năm 2017.

Điều 3. Chánh Văn phòng Uỷ ban nhân dân tỉnh, Thủ trưởng các sở, ban, ngành; Chủ tịch uỷ ban nhân dân các huyện, thành phố; Chủ tịch uỷ ban nhân dân các xã, phường, thị trấn và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Bộ Thông tin và Truyền thông (để b/c);
- TTTU, HĐND tỉnh (để b/c);
- Chủ tịch, các PCT UBND tỉnh;
- Cục Kiểm tra văn bản Bộ Tư pháp;
- Như Điều 3;
- Lưu: VT, TH.

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

Vũ Đại Thắng

ỦY BAN NHÂN DÂN TỈNH HÀ NAM	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

DỰ THẢO

QUY CHẾ

Đảm bảo an toàn thông tin trên máy tính, mạng máy tính và các thiết bị công nghệ thông tin trong hoạt động của các cơ quan nhà nước tỉnh Hà Nam

(Ban hành kèm theo Quyết định số: /2017/QĐ-UBND ngày tháng 7 năm 2017 của Uỷ ban nhân dân tỉnh Hà Nam)

Chương I

NHỮNG QUY ĐỊNH CHUNG

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

1. Quy chế này quy định về đảm bảo an toàn thông tin (ATTT) trên máy tính, mạng máy tính và các thiết bị công nghệ thông tin (CNTT) trong hoạt động ứng dụng CNTT của các cơ quan nhà nước trên địa bàn tỉnh Hà Nam.

2. Quy chế này áp dụng đối với:

- Các sở, ban, ngành, UBND huyện, thành phố và các đơn vị sự nghiệp trực thuộc UBND tỉnh; UBND các xã, phường, thị trấn (sau đây gọi tắt là cơ quan, đơn vị).

- Các tổ chức, cá nhân có tham gia quản lý, vận hành, khai thác và sử dụng các ứng dụng CNTT trong hoạt động của các cơ quan nhà nước của tỉnh.

Điều 2. Các nguyên tắc chung về đảm bảo ATTT

1. Các hoạt động ứng dụng CNTT phải tuân theo nguyên tắc đảm bảo ATTT 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 cơ quan nhà nước.

2. Áp dụng Quy chế này nhằm giảm thiểu các nguy cơ gây mất ATTT trên máy tính, mạng máy tính và các thiết bị CNTT trong các cơ quan, đơn vị.

3. Xử lý sự cố ATTT trên máy tính, mạng máy tính và các thiết bị CNTT phải đảm bảo quyền lợi hợp pháp của các tổ chức, cá nhân, không xâm phạm đời sống riêng tư, bí mật cá nhân, thông tin của cơ quan, đơn vị.

4. Các tài liệu có nội dung thuộc danh mục bí mật nhà nước không được truyền trên mạng mà phải được quản lý theo chế độ mật đúng quy định của pháp luật hiện hành.

5. Nghiêm cấm việc sử dụng máy tính kết nối Internet, thiết bị lưu trữ di động, thiết bị di động thông minh để tạo lập, lưu giữ tài liệu có nội dung mật.

Các thiết bị viễn thông, máy tính được sử dụng soạn thảo, lưu giữ tài liệu có nội dung mật phải được kiểm tra, chứng nhận của cơ quan chức năng trước khi đưa vào sử dụng.

6. Các thiết bị viễn thông, máy tính có chứa tài liệu của cơ quan nhà nước khi đưa đi công tác nước ngoài phải thực hiện theo quy định của pháp luật về bảo vệ bí mật của nhà nước.

7. Tổ chức, cá nhân không được xâm phạm ATTT trên máy tính, mạng máy tính và các thiết bị CNTT của tổ chức, cá nhân khác.

8. Thủ trưởng các cơ quan, đơn vị phải có phương án tổ chức sao lưu dữ liệu dự phòng cho mọi dữ liệu quan trọng của tỉnh, của cơ quan, đơn vị và chịu trách nhiệm nếu để xảy ra mất mát dữ liệu do không tiến hành sao lưu dự phòng.

9. Để phục vụ hoạt động theo dõi, giám sát, phân tích và điều tra, các cơ quan đơn vị phải thực hiện việc lưu trữ nhật ký hoạt động của các hệ thống tại các máy chủ (hệ điều hành và các phần mềm ứng dụng) trong thời gian ít nhất là 30 ngày.

10. Hoạt động ATTT máy tính, mạng máy tính và các thiết bị CNTT phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.

Chương II

QUY ĐỊNH ĐẢM BẢO ATTT

Điều 3. Quản lý gửi thông tin

1. Việc gửi, nhận thông tin trên máy tính, mạng máy tính và các thiết bị CNTT phải đảm bảo các yêu cầu sau đây:

a) Không giả mạo nguồn gốc gửi thông tin.

b) Tuân thủ quy định của Luật ATTT mạng và các quy định khác của pháp luật có liên quan.

2. Các cơ quan, đơn vị phải sử dụng hộp thư điện tử công vụ với địa chỉ tên miền "hanam.gov.vn" được cấp phát để trao đổi thông tin, văn bản điện tử trong quá trình xử lý công việc. Không sử dụng các hộp thư khác như gmail, yahoo...vv.

3. Việc gửi văn bản qua hệ thống phần mềm Quản lý văn bản và điều hành; Một cửa điện tử và Dịch vụ công trực tuyến; các phần mềm chuyên ngành khác phải sử dụng loại văn bản đã có dấu, chữ ký được quét (scan) dưới dạng tệp tin định dạng *.PDF và ký số trước khi gửi.

Điều 4. Quản lý phòng máy chủ

1. Các thiết bị mạng quan trọng như tường lửa (firewall), thiết bị định tuyến (router) hệ thống máy chủ... phải được đặt trong phòng máy chủ có các biện pháp bảo vệ, ngăn chặn xâm nhập trái phép vào phòng máy chủ.

2. Phòng máy chủ của các cơ quan, đơn vị là khu vực hạn chế tiếp cận. Chỉ có người có trách nhiệm theo quy định của Thủ trưởng cơ quan, đơn vị mới được phép vào phòng máy chủ.

3. Quá trình ra, vào phòng máy chủ phải được ghi chép vào sổ nhật ký quản lý phòng máy chủ.

4. Cán bộ quản lý phòng máy chủ phải thường xuyên theo dõi, bảo đảm an toàn môi trường vật lý (nhiệt độ, độ ẩm, ánh sáng,...) cho phòng máy chủ, các hệ thống hỗ trợ như: máy điều hòa, nguồn điện, đường truyền cáp quang, hệ thống báo cháy phải luôn trong tình trạng hoạt động tốt.

5. Thủ trưởng các cơ quan, đơn vị phải chỉ đạo các bộ phận chức năng có biện pháp bảo vệ đối với phòng máy chủ nhằm phòng, chống nguy cơ do cháy nổ, ngập lụt, động đất và các thảm họa khác do thiên nhiên và con người gây ra.

Điều 5. Phòng chống mã độc, Virus

1. Các hệ thống thông tin quan trọng như: Cổng Thông tin điện tử, thư điện tử, Quản lý văn bản và điều hành, Một cửa điện tử và Dịch vụ công trực tuyến... phải thường xuyên cập nhật phiên bản mới, bản vá lỗi, phần mềm nhằm kịp thời phát hiện, loại trừ các mã độc, Virus máy tính.

2. Tất cả các máy tính kết nối mạng tại các cơ quan, đơn vị phải được cài đặt, trang bị phần mềm chống mã độc, Virus và thiết lập chế độ tự động cập nhật các mẫu mã độc, Virus mới; chế độ tự động quét khi mở các tập tin.

3. Cán bộ, công chức, viên chức trong cơ quan phải được hướng dẫn về phòng chống mã độc, các rủi ro do mã độc, Virus gây ra.

4. Tất cả các tập tin phải được quét mã độc, Virus trước khi sao chép, sử dụng.

5. Tất cả các máy tính của cơ quan, đơn vị phải được cấu hình nhằm vô hiệu hóa tính năng tự động thực thi (auto play) các tệp tin trên thiết bị lưu trữ di động.

6. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến bị nhiễm mã độc, Virus trên máy tính của cơ quan, đơn vị (máy chạy chậm bất thường, cảnh báo từ phần mềm chống mã độc, mất dữ liệu...) người sử dụng phải tắt máy và báo cho cán bộ có trách nhiệm của cơ quan, đơn vị để xử lý.

Điều 6. Sao lưu dữ liệu dự phòng

1. Các dữ liệu quan trọng của cơ quan, đơn vị phải được sao lưu bao gồm: Thông tin cấu hình của hệ thống mạng, máy chủ; phần mềm ứng dụng và cơ sở dữ liệu; tập tin ghi nhật ký.

2. Các cơ quan, đơn vị phải lập kế hoạch và thực hiện sao lưu dữ liệu phù hợp với điều kiện từng cơ quan, đơn vị đảm bảo phục hồi dữ liệu ngay sau khi có sự cố xảy ra.

Điều 7. Quản lý thiết bị tường lửa

1. Hệ thống mạng máy tính của cơ quan, đơn vị phải được trang bị tường lửa để ngăn chặn và phát hiện các thâm nhập trái phép vào hệ thống mạng.

2. Nhật ký hoạt động của thiết bị tường lửa phải được lưu giữ an toàn để phục vụ công tác kiểm tra, điều tra khi có sự cố xảy ra.

Điều 8. Quản lý nhật ký vận hành các hệ thống thông tin

1. Các cơ quan, đơn vị phải thực hiện việc ghi nhật ký (log file) trên các thiết bị mạng máy tính, phần mềm ứng dụng, hệ điều hành, cơ sở dữ liệu nhằm đảm bảo các sự kiện xảy ra trên hệ thống đều được ghi nhận và lưu giữ.

2. Nhật ký phải được bảo vệ an toàn nhằm phục vụ công tác kiểm tra, phân tích khi cần thiết.

3. Các sự kiện tối thiểu cần được ghi nhật ký gồm: quá trình đăng nhập hệ thống; tạo, cập nhật, xóa dữ liệu; các hành vi xem, cấu hình hệ thống; thiết lập các kết nối vào, ra hệ thống; thay đổi quyền truy cập hệ thống.

4. Cán bộ chuyên trách CNTT của các cơ quan, đơn vị thường xuyên theo dõi bản ghi nhật ký hệ thống và các sự kiện khác có liên quan để đánh giá, báo cáo các rủi ro và mức độ nghiêm trọng các rủi ro đó.

Điều 9. Quản lý truy cập

1. Các quy định về quản lý truy cập vào hệ thống thông tin, mạng máy tính, thiết bị, phần mềm của cơ quan, đơn vị phải chi tiết và tổ chức thực hiện nghiêm túc, phù hợp với các quy định của pháp luật về ATTT.

2. Mỗi tài khoản truy cập các hệ thống thông tin chỉ được cấp cho một người quản lý và sử dụng.

3. Cán bộ, công chức, viên chức chỉ được phép truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình, có trách nhiệm bảo mật tài khoản truy cập thông tin.

4. Các hệ thống thông tin cần giới hạn số lần đăng nhập sai liên tiếp vào hệ thống. Hệ thống tự động khóa tài khoản trong một khoảng thời gian nhất định trước khi cho đăng nhập lại.

5. Tất cả các máy chủ, máy trạm phải được đặt mật khẩu truy cập và thiết lập chế độ tự khóa sau 1 thời gian nhất định không sử dụng.

6. Khi triển khai lắp đặt các thiết bị: router, switch, wifi... phải thiết lập mật khẩu mới thay cho mật khẩu mặc định của thiết bị.

7. Khi thiết lập mạng không dây trong nội bộ cơ quan, đơn vị phải cài đặt mật khẩu truy cập vào mạng và chỉ cho phép truy cập vào mạng Internet.

8. Mật khẩu đăng nhập vào hệ thống thông tin phải đảm bảo độ phức tạp cao

(có ít nhất 8 ký tự bao gồm ký tự thường, ký tự số và ký hiệu đặc biệt). Đối với hệ thống phần mềm mới đưa vào sử dụng phải tiến hành đổi mật khẩu người dùng ngay khi được cấp, tiếp nhận tài khoản. Định kỳ thay đổi mật khẩu (ít nhất 30 ngày đổi một lần), không đặt chế độ ghi nhớ mật khẩu khi sử dụng.

9. Cán bộ chuyên trách CNTT của các cơ quan, đơn vị phải thực hiện hủy tài khoản, quyền truy cập hệ thống các hệ thống thông tin, thu hồi lại tất cả các tài sản liên quan đến hệ thống thông tin (khóa, thẻ nhận dạng, thư mục lưu trữ, thư điện tử, chữ ký số, máy vi tính...) đối với các cá nhân nghỉ việc, chuyển công tác.

Điều 10. Quản lý thiết bị

1. Thiết bị CNTT đặt tại phòng máy chủ của các cơ quan, đơn vị phải đặt tên và dán nhãn đúng quy định.

2. Khi sửa chữa các thiết bị CNTT, hạn chế cho phép mang thiết bị, nhất là thiết bị lưu trữ dữ liệu ra khỏi cơ quan, đơn vị và bố trí cán bộ giám sát.

3. Khi thanh lý tài sản là thiết bị CNTT có lưu trữ dữ liệu, phải xóa dữ liệu để không thể phục hồi nhằm đảm bảo bí mật các dữ liệu có trên các thiết bị đó.

Điều 11. Quản lý bản quyền phần mềm

1. Các phần mềm, chương trình ứng dụng sử dụng cho máy chủ tại các cơ quan, đơn vị nếu là phần mềm mã nguồn đóng thì phải có bản quyền sử dụng theo đúng quy định của pháp luật. Khuyến khích sử dụng các phần mềm mã nguồn mở.

2. Cán bộ, công chức, viên chức và người lao động trong các cơ quan, đơn vị không phát tán chia sẻ phần mềm có bản quyền đã được đầu tư, cấp phát cho các đối tượng ngoài cơ quan, đơn vị với mục đích ngoài nhiệm vụ chuyên môn được giao.

Điều 12. An toàn cho máy tính cá nhân (máy tính để bàn, máy tính xách tay)

1. Cài đặt phần mềm diệt Virus, mã độc cho tất cả các máy tính trong mạng LAN của cơ quan, đơn vị. Thiết lập chế độ cập nhật hàng ngày cho phần mềm diệt Virus, mã độc.

2. Thủ trưởng các cơ quan, đơn vị phải quán triệt cán bộ, công chức, viên chức không được cài đặt phần mềm không rõ nguồn gốc, xuất xứ; không truy cập các trang web có nội dung không lành mạnh; không mở những thư điện tử không rõ địa chỉ người gửi... nhằm tránh tối đa việc phần mềm Virus, mã độc tự động cài đặt vào máy tính cá nhân.

3. Mã hóa phân vùng ổ cứng chứa dữ liệu quan trọng trên các máy tính cá nhân; đặt mật khẩu mở các tệp tài liệu khi gửi trên môi trường mạng trong các trường hợp cần thiết.

4. Không chia sẻ thư mục trên mạng LAN theo cơ chế cho phép toàn quyền đọc, ghi (Share Full), chỉ thiết lập cơ chế chỉ đọc (Read Only) và yêu cầu sử dụng mật khẩu khi truy cập thư mục chia sẻ.

Điều 13. An toàn khi sử dụng các thiết bị lưu trữ ngoài

1. Việc sử dụng các thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB,... phải quét Virus, mã độc trước khi đọc hoặc sao chép dữ liệu.

2. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu.

Điều 14. Soạn thảo nội dung thuộc bí mật nhà nước

1. Thủ trưởng cơ quan, đơn vị phải nghiên cứu, xác định độ mật của các văn bản có nội dung thuộc danh mục bí mật nhà nước do cơ quan, đơn vị, địa phương ban hành để quản lý theo đúng quy định.

2. Đảm bảo an toàn khi sử dụng máy tính cho soạn thảo văn bản có nội dung thuộc bí mật nhà nước, các cơ quan đơn vị cần bố trí 01 máy tính dùng riêng có đặt mật khẩu bảo vệ và không kết nối với mạng LAN, Internet theo đúng quy định về soạn thảo các văn bản có tính chất Mật.

Điều 15. Quản lý sự cố

1. Phân loại mức độ nghiêm trọng của các sự cố, bao gồm:

a) Thấp: sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan, đơn vị.

b) Trung bình: sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của cơ quan, đơn vị.

c) Cao: sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và gây ảnh hưởng đến một trong các hoạt động chính của cơ quan, đơn vị.

d) Khẩn cấp: sự cố ảnh hưởng đến hoạt động của nhiều hoạt động chính của cơ quan, đơn vị.

2. Khi có sự cố hay nguy cơ gây mất ATTT, Thủ trưởng cơ quan, đơn vị phải chỉ đạo kịp thời để khắc phục và hạn chế các thiệt hại, báo cáo nhanh qua điện thoại, thư điện tử và bằng văn bản cho đơn vị chuyên trách CNTT, Sở Thông tin và Truyền thông.

3. Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp vượt quá khả năng khắc phục của cơ quan, đơn vị, thủ trưởng cơ quan, đơn vị phải báo cáo ngay cho Sở Thông tin và Truyền thông để có phương án hỗ trợ, khắc phục.

Chương III
TRÁCH NHIỆM ĐẢM BẢO ATTT

Điều 16. Trách nhiệm của Sở Thông tin và Truyền thông

1. Tham mưu với UBND tỉnh về công tác đảm bảo ATTT trên địa bàn tỉnh và chịu trách nhiệm trước UBND tỉnh trong việc đảm bảo an toàn cho các hệ thống thông tin dùng chung của tỉnh như: Cổng Thông tin điện tử, thư điện tử, Quản lý văn bản và Điều hành.

2. Chịu trách nhiệm xây dựng và trình UBND tỉnh hoặc trình HĐND tỉnh ban hành các cơ chế, chính sách và hướng dẫn, khuyến nghị về đảm bảo ATTT cho các cơ quan, đơn vị.

3. Tham mưu với UBND tỉnh hướng dẫn việc sử dụng các thiết bị CNTT để lưu giữ và truyền tải thông tin bí mật nhà nước.

4. Nghiên cứu, tham mưu với UBND tỉnh xây dựng đội ngũ cán bộ chuyên trách về ATTT có trình độ đáp ứng yêu cầu theo quy định; tổ chức bộ phận chuyên trách về ATTT có trách nhiệm đảm bảo ATTT cho các hệ thống CNTT dùng chung của tỉnh và hỗ trợ các cơ quan, đơn vị trong tỉnh xử lý sự cố.

5. Chủ trì, phối hợp Công an tỉnh và các cơ quan, đơn vị có liên quan định kỳ hàng năm tiến hành công tác thanh tra, kiểm tra, đánh giá công tác đảm bảo ATTT và xử lý các hành vi vi phạm ATTT tại các cơ quan nhà nước trên địa bàn tỉnh. Tổ chức kiểm tra đột xuất các cơ quan, đơn vị khi có dấu hiệu vi phạm ATTT.

6. Hàng năm xây dựng kế hoạch, chương trình, dự án, tổng hợp kinh phí để triển khai công tác ATTT trong hoạt động ứng dụng CNTT của các cơ quan, đơn vị trên địa bàn tỉnh.

7. Thẩm định về ATTT trong hồ sơ thiết kế hệ thống thông tin của các cơ quan, đơn vị trên địa bàn tỉnh.

8. Xây dựng và triển khai các chương trình đào tạo, hội nghị tuyên truyền ATTT trong công tác quản lý nhà nước trên địa bàn tỉnh.

9. Hướng dẫn cụ thể về nghiệp vụ quản lý vận hành, kỹ thuật đảm bảo ATTT; hỗ trợ các cơ quan, đơn vị giải quyết sự cố ATTT khi có yêu cầu.

10. Thiết lập đường dây nóng, bố trí cán bộ thường trực để tiếp nhận các phản ánh của các cơ quan, đơn vị về nguy cơ gây mất ATTT; phối hợp hướng dẫn, xử lý kịp thời.

11. Thông báo cho các cơ quan, đơn vị biết và có biện pháp phòng ngừa, ngăn chặn rủi ro, các nguy cơ mất ATTT do Virus, phần mềm độc hại, phần mềm gián điệp gây ra.

12. Định kỳ 6 tháng, hàng năm, hoặc đột xuất tổng hợp báo cáo UBND tỉnh về tình hình đảm bảo ATTT trong các cơ quan nhà nước tỉnh Hà Nam.

Điều 17. Trách nhiệm của Công an tỉnh

1. Điều tra và xử lý các trường hợp vi phạm ATTT theo thẩm quyền.

2. Phối hợp Sở Thông tin và Truyền thông kiểm tra công tác ATTT đối với các cơ quan, đơn vị trên địa bàn tỉnh.

3. Thường xuyên thông báo cho các cơ quan, đơn vị về phương thức, thủ đoạn của các loại tội phạm ATTT để có biện pháp phòng ngừa, phát hiện, đấu tranh, ngăn chặn.

4. Thực hiện nhiệm vụ bảo vệ an toàn các công trình quan trọng về an ninh của quốc gia, của tỉnh trên lĩnh vực CNTT.

Điều 18. Trách nhiệm của Sở Tài chính

Phối hợp với Sở Thông tin và Truyền thông tham mưu UBND tỉnh bố trí kinh phí sự nghiệp hàng năm và kinh phí thực hiện các nhiệm vụ đột xuất phục vụ các hoạt động đảm bảo ATTT trong các cơ quan, đơn vị trên địa bàn tỉnh.

Điều 19. Trách nhiệm của Sở Kế hoạch và Đầu tư

Chủ trì phối hợp với Sở Thông tin và Truyền thông, Sở Tài chính tổng hợp, tham mưu ưu tiên bố trí nguồn vốn ngân sách trong kế hoạch chi đầu tư phát triển hàng năm để thực hiện các dự án đầu tư đảm bảo ATTT cho các cơ quan, đơn vị trên địa bàn tỉnh.

Điều 20. Trách nhiệm của đơn vị chuyên trách CNTT trong ứng cứu sự cố thông tin

Đơn vị chuyên trách CNTT là Trung tâm Công nghệ thông tin và Truyền thông tỉnh Hà Nam có trách nhiệm như sau:

1. Tham mưu với UBND tỉnh chỉ đạo tổ chức triển khai công tác đảm bảo ATTT trên máy tính, mạng máy tính và các thiết bị CNTT đối với các cơ quan, đơn vị trên địa bàn tỉnh.

2. Hỗ trợ các cơ quan, đơn vị trên địa bàn tỉnh trong công tác đảm bảo ATTT trong hoạt động ứng dụng CNTT và tổ chức ứng cứu các sự cố mạng, máy tính.

3. Là đầu mối của tỉnh, phối hợp với Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT), các đơn vị chức năng có liên quan ngăn chặn, xử lý và khắc phục sự cố mạng, máy tính các cơ quan, đơn vị trên địa bàn tỉnh.

4. Thực hiện trách nhiệm làm đầu mối ứng cứu sự cố của tỉnh trong mạng lưới ứng cứu sự cố mạng, máy tính trên toàn quốc dưới sự điều phối của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT).

Điều 21. Trách nhiệm của các cơ quan, đơn vị

1. Thủ trưởng các cơ quan, đơn vị có trách nhiệm tổ chức quán triệt, nâng cao nhận thức cho cán bộ, công chức, viên chức về đảm bảo ATTT; tổ chức triển khai thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước

UBND tỉnh trong công tác đảm bảo ATTT của cơ quan, đơn vị mình.

2. Bảo vệ ATTT trong mạng nội bộ là trách nhiệm của các cơ quan, đơn vị quản lý mạng nội bộ đó.

3. Trang bị đầy đủ kiến thức bảo mật cơ bản cho cán bộ, công chức, viên chức về ATTT trước khi cho phép truy nhập và sử dụng Hệ thống thông tin. Bố trí, tạo điều kiện làm việc phù hợp với chuyên môn và ưu tiên bồi dưỡng nghiệp vụ về ATTT cho cán bộ chuyên trách (hoặc cán bộ được giao phụ trách) về CNTT trong các cơ quan, đơn vị. Khuyến khích các cơ quan, đơn vị liên kết với tổ chức, cá nhân, doanh nghiệp CNTT uy tín mở các khóa đào tạo nhân lực trong lĩnh vực ATTT.

4. Bố trí kinh phí cho việc mua sắm, nâng cấp các trang thiết bị phần cứng, phần mềm để đảm bảo và tăng cường ATTT trong hoạt động ứng dụng CNTT của cơ quan, đơn vị.

5. Khi có sự cố ATTT hoặc có nguy cơ mất ATTT phải kịp thời chỉ đạo khắc phục ngay, ưu tiên sử dụng cán bộ kỹ thuật chuyên trách trong cơ quan, đơn vị. Kịp thời báo cho doanh nghiệp cung cấp dịch vụ và thông báo bằng văn bản cho đơn vị chuyên trách CNTT, Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ xử lý.

6. Xây dựng quy chế nội bộ về đảm bảo ATTT trong cơ quan, đơn vị mình.

7. Khi triển khai đầu tư ứng dụng CNTT phải có phương án đảm bảo ATTT từ khâu thiết kế và phải tự chịu trách nhiệm đảm bảo ATTT cho hệ thống CNTT và các hệ thống thông tin của cơ quan, đơn vị mình.

8. Phối hợp chặt chẽ với cơ quan Công an trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm ATTT.

9. Phối hợp với Sở Thông tin và Truyền thông và các cơ quan, đơn vị liên quan thực hiện công tác kiểm tra khắc phục sự cố ATTT; đồng thời cung cấp đầy đủ các thông tin khi đoàn kiểm tra yêu cầu. Không được che giấu thông tin về sự cố nhằm gây khó khăn cho các cơ quan chức năng đánh giá thiệt hại để có phương án xử lý.

10. Báo cáo tình hình và kết quả thực hiện công tác đảm bảo ATTT tại cơ quan, đơn vị, định kỳ hàng năm (trước ngày 15/11) gửi về Sở Thông tin và Truyền thông.

Điều 22. Trách nhiệm của doanh nghiệp viễn thông, CNTT cung cấp hạ tầng phục vụ ứng dụng CNTT trong cơ quan nhà nước

1. Có trách nhiệm đầu tư, phát triển hạ tầng viễn thông, đường truyền phục vụ việc ứng dụng CNTT đảm bảo ATTT cho hệ thống do doanh nghiệp thiết lập.

2. Viễn thông Hà Nam có trách nhiệm đảm bảo hệ thống mạng truyền số liệu chuyên dùng của các cơ quan, đơn vị trên địa bàn tỉnh; phối hợp với Sở

Thông tin và Truyền thông trong việc xử lý khắc phục khi có sự cố trên hệ thống mạng truyền số liệu chuyên dùng của tỉnh.

Điều 23. Trách nhiệm các tổ chức, cá nhân tham gia quản lý, vận hành, khai thác ứng dụng CNTT trong các cơ quan nhà nước

1. Tuân thủ theo quy định tại Quy chế này và các quy định khác của pháp luật có liên quan.

2. Thực hiện tốt các biện pháp đảm bảo ATTT khi tương tác, sử dụng ứng dụng CNTT của các cơ quan nhà nước phục vụ người dân và doanh nghiệp.

3. Chịu trách nhiệm về các thông tin cá nhân đăng ký, khai báo khi sử dụng tương tác các ứng dụng CNTT của tỉnh; tuân thủ các hướng dẫn khi sử dụng dịch vụ CNTT của tỉnh.

4. Không thu thập, sử dụng, phát tán, quảng cáo, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống dịch vụ ứng dụng CNTT thông tin để thu thập, khai thác thông tin cá nhân.

Điều 24. 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 chuyên trách hoặc cán bộ được giao phụ trách CNTT trong các cơ quan, đơn vị:

- Chịu trách nhiệm đảm bảo ATTT của cơ quan, đơn vị.

- Chịu trách nhiệm triển khai các biện pháp quản lý, vận hành, quản lý kỹ thuật, tham mưu xây dựng quy định về đảm bảo an toàn cho hệ thống thông tin của cơ quan, đơn vị mình theo quy chế này.

- Thực hiện việc giám sát, đánh giá, báo cáo thủ trưởng cơ quan, đơn vị các rủi ro mất ATTT và mức độ nghiêm trọng của các rủi ro đó.

- Phối hợp với các cá nhân, các cơ quan, đơn vị có liên quan trong việc kiểm tra, phát hiện và khắc phục các sự cố mất ATTT.

2. Trách nhiệm của cán bộ, công chức, viên chức và người lao động

- Chấp hành nghiêm túc các quy định về ATTT của các cơ quan, đơn vị cũng như các quy định khác của pháp luật, nâng cao ý thức cảnh giác và trách nhiệm đảm bảo ATTT tại cơ quan, đơn vị.

- Khi phát hiện sự cố mất ATTT phải báo ngay với cấp trên và bộ phận chuyên trách của cơ quan, đơn vị để kịp thời ngăn chặn, xử lý. Không tự ý liên hệ với cá nhân bên ngoài vào can thiệp các thiết bị phần cứng, phần mềm của cơ quan, đơn vị mình.

- Không sử dụng hòm thư công vụ có địa chỉ tên miền "hanam.gov.vn" được cấp phát cho cá nhân hoặc cơ quan, đơn vị mình vào mục đích cá nhân như đăng ký tài khoản mạng xã hội, đăng ký mua sắm qua mạng.

Chương IV

TỔ CHỨC THỰC HIỆN

Điều 25. Khen thưởng và xử lý vi phạm

1. Hàng năm, Sở Thông tin và Truyền thông dựa trên các điều tra, báo cáo công tác ATTT của các cơ quan, đơn vị tham mưu với UBND tỉnh đưa ATTT vào tiêu chí đánh giá thi đua của các cơ quan nhà nước trên địa bàn tỉnh.

2. Các cơ quan, đơn vị, tổ chức, cá nhân có hành vi vi phạm Quy chế này tùy theo tính chất, mức độ vi phạm mà bị xử lý theo quy định của pháp luật hiện hành.

Điều 26. Điều khoản thi hành

Trong quá trình thực hiện, nếu có vướng mắc, phát sinh, các cơ quan, đơn vị kịp thời phản ánh về Sở Thông tin và Truyền thông để tổng hợp, báo cáo UBND tỉnh xem xét sửa đổi, bổ sung Quy chế cho phù hợp./.

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

Vũ Đại Thắng