ỦY BAN NHÂN DÂN **TỈNH KHÁNH HÒA**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 38 /2015/QĐ-UBND	*Nha Trang, ngày 14 tháng 12 năm 2015*

QUYẾT ĐỊNH

Ban hành Quy định đảm bảo an toàn thông tin số trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Khánh Hòa

ỦY BAN NHÂN DÂN TỈNH KHÁNH HÒA

Căn cứ Luật Tổ chức Hội đồng nhân dân và Ủy ban nhân dân ngày 26 tháng 11 năm 2003;

Căn cứ Luật Ban hành văn bản quy phạm pháp luật của Hội đồng nhân dân, Ủy ban nhân dân ngày 03 tháng 12 năm 2004;

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

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về Ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Căn cứ Nghị định số 90/2008/NĐ-CP ngày 13/08/2008 của Chính phủ về chống thư rác và Nghị định số 77/2012/NĐ-CP ngày 05/10/2012 của Chính phủ về sửa đổi, bổ sung một số điều của Nghị định số 90/2008/NĐ-CP ngày 13/08/2008 của Chính phủ về chống thư rác;

Căn cứ Quyết định số 63/QĐ-TTg ngày 13/01/2010 của Thủ tướng Chính phủ phê duyệt Quy hoạch phát triển an toàn thông tin số quốc gia đến năm 2020;

Căn cứ Chỉ thị số 897/CT-TTg ngày 10/06/2011 của Thủ tướng Chính phủ về việc tăng cường triển khai các hoạt động đảm bảo an toàn thông tin số;

Căn cứ Chỉ thị số 15/CT-TTg ngày 17/6/2014 của Thủ tướng Chính phủ về việc tăng cường công tác bảo đảm an ninh và an toàn thông tin mạng trong tình hình mới.

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình 1530/TTr-STTTT ngày 18/12/2014 và Công văn số 1518/STTTT-CNTT ngày 14/12/2015,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này, Quy định đảm bảo an toàn thông tin số trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Khánh Hòa.

Điều 2. Quyết định này có hiệu lực sau 10 (mười) ngày kể từ ngày ký và thay thế Quyết định số 36/2010/QĐ-UBND ngày 12/11/2010 của Ủy ban nhân dân tỉnh Khánh Hòa 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 quản lý hành chính nhà nước tỉnh Khánh Hòa.

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh; Giám đốc Sở Thông tin và Truyền thông; Thủ trưởng các sở, ban ngành; Chủ tịch Ủy ban nhân dân các huyện, thị xã, thành phố; Thủ trưởng các cơ quan Đảng, các tổ chức đoàn thể chính trị - xã hội thuộc tỉnh và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Ủy ban Thường vụ Quốc hội;
- Văn phòng Chính phủ;
- Bộ Thông tin và Truyền thông;
- Cục Kiểm tra văn bản - Bộ Tư pháp;
- TT.Tỉnh ủy;
- TT.HĐND tỉnh;
- Chủ tịch và các PC. UBND tỉnh;
- Đoàn đại biểu Quốc hội tỉnh Khánh Hòa;
- UB MTTQ Việt Nam tỉnh;
- Sở Tư pháp;
- Trung tâm Công báo tỉnh;
- Cổng TTĐT tỉnh;
- Đài PTTH, Báo Khánh Hòa;
- Lưu: VT, NN, QP.

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

Nguyễn Duy Bắc

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

QUY ĐỊNH
Đảm bảo an toàn thông tin số trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Khánh Hòa

(Ban hành kèm theo Quyết định số: 38 /2015/QĐ-UBND ngày 24 tháng 12 năm 2015 của Ủy ban nhân dân tỉnh Khánh Hòa)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy định này quy định về công tác đảm bảo an toàn thông tin số; trách nhiệm của các tổ chức, cá nhân trong công tác đảm bảo an toàn thông tin số trong hoạt động ứng dụng công nghệ thông tin của cơ quan hành chính nhà nước, cơ quan Đảng, Mặt trận Tổ quốc và các tổ chức đoàn thể chính trị - xã hội thuộc tỉnh Khánh Hòa.

Điều 2. Đối tượng áp dụng

1. Quy định này áp dụng đối với cơ quan hành chính nhà nước, các đơn vị sự nghiệp sử dụng ngân sách nhà nước, cơ quan Đảng, Mặt trận và các tổ chức đoàn thể chính trị - xã hội thuộc tỉnh Khánh Hòa (sau đây gọi là cơ quan).

2. Cán bộ, công chức, viên chức, người lao động đang làm việc trong các cơ quan nêu tại Khoản 1 Điều này (sau đây gọi là người sử dụng) và các tổ chức, cá nhân có liên quan.

Điều 3. Giải thích từ ngữ

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

1. *Hệ thống thông tin:* Là một hệ thống sử dụng công nghệ thông tin để thu thập, truyền, lưu trữ, xử lý và cung cấp thông tin phục vụ nhu cầu sử dụng của các tổ chức, cá nhân.

2. *An toàn thông tin số:* Bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin đối với nguy cơ tự nhiên hoặc do con người gây ra.

3. *Cán bộ chuyên trách công nghệ thông tin*: Là công chức, viên chức làm việc trong các cơ quan được giao trách nhiệm tham mưu công tác quản lý và trực tiếp thực hiện nhiệm vụ quản trị hệ thống thông tin của cơ quan.

Điều 4. Hệ thống thông tin của cơ quan

1. Hệ thống thông tin của cơ quan được xây dựng để phục vụ hoạt động của cơ quan, bao gồm: Cơ sở hạ tầng thông tin của cơ quan; các phần mềm ứng dụng, dữ

liệu, thông tin được tạo ra, lưu trữ, trao đổi và sử dụng trên cơ sở hạ tầng thông tin của cơ quan.

2. Hệ thống thông tin của các cơ quan phải tuân thủ các nguyên tắc đảm bảo an toàn thông tin số theo quy định tại Điều 41 Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về Ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước.

3. Thủ trưởng cơ quan là người có quyền cao nhất đối với toàn bộ hoạt động và công tác đảm bảo an toàn thông tin số cho hệ thống thông tin của cơ quan; có toàn quyền trong việc giao hay không giao quyền sử dụng, thu hồi quyền của người sử dụng trong hệ thống thông tin của cơ quan; có quyền quyết định việc sử dụng các thành phần của hệ thống thông tin ngoài mục đích phục vụ công việc trên cơ sở tuân thủ các quy định của pháp luật và chịu hoàn toàn trách nhiệm đối với quyết định của mình.

4. Hệ thống thông tin của các cơ quan Đảng, Mặt trận Tổ quốc và các tổ chức đoàn thể chính trị - xã hội phải tuân thủ các nguyên tắc về bảo mật, an toàn, an ninh thông tin do Ban Chỉ đạo công nghệ thông tin cơ quan Đảng, Văn phòng Trung ương Đảng quy định.

Chương II
QUY ĐỊNH QUẢN LÝ HỆ THỐNG THÔNG TIN ĐẢM BẢO AN TOÀN THÔNG TIN SỐ

Điều 5. Quy định quản lý vận hành hệ thống thông tin đảm bảo an toàn thông tin số

1. Các cơ quan, đơn vị phải trang bị đầy đủ các kiến thức bảo mật cơ bản cho người sử dụng trước khi cho phép truy cập và sử dụng hệ thống thông tin.

2. Cán bộ chuyên trách công nghệ thông tin của cơ quan phải được đảm bảo điều kiện học tập, tiếp thu công nghệ, kiến thức an toàn bảo mật thông tin phục vụ việc tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ.

3. Các cơ quan phải xây dựng bộ tài liệu kỹ thuật mô tả toàn bộ kiến trúc mạng, thông số kỹ thuật, cấu hình hệ thống, giải pháp sao lưu và phục hồi dữ liệu cho máy chủ, máy trạm và thiết bị mạng trong hệ thống thông tin của cơ quan mình.

4. Hệ thống thông tin của các cơ quan cấp huyện và cấp tỉnh phải có trang bị công cụ tường lửa và giám sát truy cập cho hệ thống mạng.

5. Các cơ quan phải tổ chức thực hiện các biện pháp quản lý vận hành sau đây đối với hệ thống thông tin tại cơ quan mình:

a) Thực hiện các biện pháp sao lưu cấu hình, trạng thái, ứng dụng, dữ liệu của hệ thống thông tin và lưu trữ dữ liệu sao lưu tại nơi an toàn, đồng thời, dữ liệu sao lưu phải được tổ chức kiểm tra và cập nhật thường xuyên để phục vụ công tác tra cứu, phục hồi trong trường hợp cần thiết;

b) Triển khai các biện pháp phòng, chống phần mềm có hại (virus, worm, spyware,...) cho những thành phần quan trọng của hệ thống (tường lửa, máy chủ, thiết bị mạng,...) và tại các máy trạm; đồng thời thường xuyên cập nhật cơ chế phòng, chống phần mềm có hại phù hợp với quy trình và chính sách quản lý cấu hình hệ thống thông tin của cơ quan;

c) Thực hiện kiểm tra, giám sát toàn bộ hệ thống thông tin của cơ quan ít nhất 01 lần/01 năm nhằm rà soát, kiểm tra, đánh giá, phát hiện những nguy cơ hoặc sự cố gây mất an toàn thông tin số; đồng thời tổ chức thực hiện các biện pháp phòng ngừa, ngăn chặn, xử lý cần thiết, kịp thời nhằm hạn chế mức độ ảnh hưởng và gây thiệt hại đối với hệ thống thông tin hoặc tài sản, uy tín của cơ quan;

d) Thực hiện hủy quyền truy cập hệ thống thông tin và thu hồi các tài sản liên quan tới hệ thống thông tin (khóa, thẻ tài khoản, thẻ nhận dạng,...) của người sử dụng đã nghỉ hưu, nghỉ việc hoặc chuyển công tác đến cơ quan khác, nhưng vẫn đảm bảo khả năng truy cập vào các hồ sơ, tài liệu được tạo ra bởi cán bộ, công chức hoặc nhân viên đó;

đ) Các biện pháp khác theo hướng dẫn của cơ quan quản lý chuyên ngành.

6. Các cơ quan quan tâm phân bổ đầu tư cần thiết để đảm bảo và tăng cường an toàn thông tin số trong hoạt động ứng dụng công nghệ thông tin của cơ quan mình.

Điều 6. Quy định quản lý kỹ thuật hệ thống thông tin đảm bảo an toàn thông tin số

1. Hệ thống thông tin của các cơ quan phải được thiết lập cấu hình theo những nguyên tắc sau:

a) Chỉ cung cấp những chức năng thiết yếu nhất cho người sử dụng theo yêu cầu quản lý và sử dụng hệ thống thông tin phục vụ công việc;

b) Các thành phần của hệ thống thông tin phải được thường xuyên cập nhật cấu hình chuẩn theo hướng dẫn, khuyến nghị của nhà sản xuất thiết bị, đơn vị cung cấp phần mềm ứng dụng hoặc cơ quan quản lý nhà nước chuyên ngành;

c) Thực hiện cấm hoặc hạn chế sử dụng các chức năng, cổng giao tiếp, giao thức và dịch vụ mạng không cần thiết nhưng vẫn đảm bảo duy trì hoạt động thường xuyên của hệ thống thông tin.

2. Các cơ quan phải tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin của cơ quan.

3. Các cơ quan phải tổ chức quản lý các tài khoản của hệ thống thông tin, bao gồm: Tạo mới, kích hoạt, sửa đổi, vô hiệu hóa và loại bỏ các tài khoản, đồng thời tổ chức kiểm tra các tài khoản của hệ thống thông tin ít nhất 01 lần/01 năm và triển khai các công cụ tự động để hỗ trợ việc quản lý các tài khoản của hệ thống thông tin.

4. Các cơ quan phải triển khai các biện pháp quản lý truy cập vào hệ thống thông tin, bao gồm:

a) Thiết lập cơ chế giới hạn một số hữu hạn lần (không quá 05 lần) đăng nhập sai liên tiếp vào các thành phần của hệ thống thông tin. Nếu liên tục đăng nhập sai

vượt quá số lần quy định thì hệ thống phải tự động khóa tài khoản trong một khoảng thời gian nhất định;

b) Thực hiện theo dõi, giám sát, điều khiển tất cả các kết nối truy cập từ xa và ngăn chặn tất cả các kết nối truy cập từ xa trái phép vào hệ thống thông tin của cơ quan;

c) Sử dụng chứng thực và mã hóa để bảo vệ truy cập không dây tới hệ thống thông tin của cơ quan, đồng thời triển khai các biện pháp theo dõi, giám sát, điều khiển, cho phép, hạn chế hoặc ngăn chặn các truy cập mạng không dây trái phép;

d) Ghi nhận và lưu giữ trong một khoảng thời gian nhất định các sự kiện về quá trình đăng nhập, cấu hình, truy xuất hệ thống và các thông tin liên quan vào các bản ghi nhật ký nhằm xác định những sự kiện đã xảy ra, nguồn gốc và các kết quả của sự kiện đó để có cơ chế bảo vệ an toàn thông tin số hiệu quả cho hệ thống thông tin của cơ quan;

đ) Các biện pháp khác theo hướng dẫn của cơ quan quản lý chuyên ngành.

5. Hệ thống thông tin tại các cơ quan, đơn vị phải có cơ chế ngăn chặn hoặc hạn chế các sự cố gây ra do tấn công từ chối dịch vụ bằng cách sử dụng các thiết bị đặt tại biên của mạng để lọc các gói tin nhằm bảo vệ các thiết bị bên trong, tránh bị ảnh hưởng trực tiếp bởi tấn công từ chối dịch vụ.

Điều 7. Xây dựng quy định và quy trình nội bộ về đảm bảo an toàn thông tin số

1. Các cơ quan phải ban hành quy định nội bộ về đảm bảo an toàn thông tin số, đảm bảo quy định rõ các vấn đề sau:

a) Mục tiêu và phương hướng thực hiện công tác đảm bảo an toàn số;

b) Nguyên tắc phân loại và quản lý mức độ ưu tiên đối với các thành phần của hệ thống thông tin (phần mềm, dữ liệu, trang thiết bị);

c) Nguyên tắc chung về sử dụng an toàn và hiệu quả đối với các cá nhân tham gia sử dụng hệ thống thông tin;

d) Quy định về quản lý phân quyền và trách nhiệm đối với từng cá nhân khi tham gia sử dụng hệ thống thông tin;

đ) Quy định về quản lý và điều hành hệ thống máy chủ, thiết bị mạng, thiết bị bảo vệ mạng một cách an toàn;

e) Công tác kiểm tra, rà soát và khắc phục sự cố mất an toàn thông tin số cho hệ thống bằng cách sử dụng các biện pháp trong Điều 5 và Điều 6 của Quy định này;

g) Báo cáo tổng hợp tình hình thực hiện công tác đảm bảo an toàn thông tin số của hệ thống theo định kỳ;

h) Các biện pháp tổ chức thực hiện.

2. Các cơ quan phải xây dựng và áp dụng quy trình đảm bảo an toàn thông tin số cho hệ thống thông tin của mình nhằm giảm thiểu các nguy cơ gây sự cố, tạo điều

kiện cho việc khắc phục và truy vết trong trường hợp có sự cố xảy ra. Nội dung của quy trình có thể chia làm các bước cơ bản như sau:

a) Lập kế hoạch bảo vệ an toàn thông tin số cho hệ thống thông tin;

b) Xây dựng hệ thống bảo vệ an toàn thông tin số;

c) Quản lý và vận hành hệ thống bảo vệ an toàn thông tin số;

d) Kiểm tra đánh giá hoạt động hệ thống bảo vệ an toàn thông tin số;

đ) Bảo trì và nâng cấp hệ thống bảo vệ an toàn thông tin số.

3. Khuyến khích các cơ quan xây dựng và áp dụng Hệ thống quản lý an toàn thông tin theo Tiêu chuẩn quốc gia TCVN ISO/IEC 27001:2009 do Bộ Khoa học và Công nghệ ban hành năm 2009 đối với hệ thống thông tin của cơ quan mình.

Chương III
QUY ĐỊNH SỬ DỤNG HỆ THỐNG THÔNG TIN ĐẢM BẢO AN TOÀN THÔNG TIN SỐ

Điều 8. Đảm bảo an toàn thông tin số trong việc kết nối và truy cập mạng Internet

1. Kết nối hệ thống thông tin của các cơ quan với mạng Internet (để sử dụng các dịch vụ cung cấp qua mạng Internet, cung cấp thông tin và dịch vụ công cho tổ chức, cá nhân theo quy định của pháp luật) là tài sản nhà nước cấp cho người sử dụng với mục đích phục vụ công việc chuyên môn.

2. Các cơ quan phải thực hiện kiểm soát, hạn chế, không cho phép hoặc xem xét kỷ luật đối với người sử dụng dùng kết nối Internet của cơ quan để sử dụng các dịch vụ làm tiêu tốn nhiều thời gian, băng thông kết nối Internet phục vụ cho mục đích cá nhân trong giờ làm việc hành chính (như các dạng tải dữ liệu dung lượng lớn, kết nối mạng và chuyển dữ liệu trực tiếp với máy tính bên ngoài hệ thống thông tin, trao đổi trực tuyến có sử dụng giao tiếp âm thanh và hình ảnh,...).

3. Hệ thống thông tin của các cơ quan phải được triển khai các biện pháp cấm truy cập các cổng/trang thông tin điện tử, diễn đàn, mạng xã hội, địa chỉ trực tuyến hoặc các mạng thông tin khác có nội dung không phù hợp; không cho phép tải về hoặc đưa lên mạng Internet một số định dạng dữ liệu nếu việc tải về hoặc đưa lên mạng Internet các định dạng dữ liệu đó không phục vụ cho công việc. Việc áp dụng các biện pháp này có thể thực hiện mà không cần thông báo trước.

4. Các hành vi bị nghiêm cấm trong quá trình sử dụng kết nối mạng Internet của cơ quan:

a) Truy cập và phát tán các nội dung trái quy định của pháp luật;

b) Sử dụng kết nối Internet của cơ quan để tải về hoặc sử dụng phim trực tuyến, nhạc trực tuyến, trò chơi trực tuyến trong giờ làm việc hành chính;

c) Chia sẻ hoặc tự ý cho người ngoài cơ quan sử dụng kết nối mạng Internet của cơ quan, sử dụng kết nối mạng Internet của cơ quan ngoài mục đích phục vụ công việc khi chưa được thủ trưởng cơ quan cho phép.

5. Các cơ quan Đảng, Mặt trận và các tổ chức đoàn thể chính trị - xã hội có kết nối với Mạng Thông tin diện rộng của Đảng phải tuân thủ đầy đủ các quy định, hướng dẫn về bảo mật, an toàn, an ninh thông tin do Trung ương, Tỉnh ủy quy định khi quy cập, khai thác sử dụng thông tin trên mạng.

Điều 9. Đảm bảo an toàn thông tin số trong việc sử dụng máy tính cá nhân

1. Máy tính cá nhân do cơ quan cấp cho người sử dụng để phục vụ công việc và được quản lý theo các quy định của pháp luật về quản lý tài sản nhà nước.

2. Các cơ quan phải quy định cụ thể các chương trình, phần mềm được phép cài đặt trên các máy tính cá nhân của cơ quan phục vụ công việc của từng nhóm người sử dụng (văn thư, chuyên viên, kế toán,...) và tổ chức thực hiện cài đặt các phần mềm này cho người sử dụng.

3. Các cơ quan phải tổ chức thực hiện các biện pháp cơ bản sau nhằm đảm bảo an toàn thông tin số cho các máy tính cá nhân của cơ quan:

a) Cài đặt và sử dụng các phần mềm, hệ điều hành có bản quyền;

b) Thường xuyên cập nhật các bản vá bảo mật cho phần mềm và hệ điều hành;

c) Cài đặt các phần mềm chống phần mềm có hại, kiểm tra toàn bộ thông tin, dữ liệu, tập tin ngay khi được tải về hoặc trước khi sao chép, lưu trữ vào máy tính;

d) Cài đặt tường lửa cá nhân để chặn các truy cập từ bên ngoài trái với quy định của cơ quan;

đ) Cấu hình máy tính cá nhân để mỗi người sử dụng chỉ được phép truy cập các thư mục lưu trữ dữ liệu của mình, không truy cập các thư mục lưu trữ dữ liệu của cá nhân khác trên máy tính dùng chung;

e) Sử dụng chức năng mã hoá dữ liệu, khóa thư mục để đề phòng trường hợp dữ liệu bị đánh cắp;

g) Hiển thị đầy đủ phần mở rộng của tập tin để không kích hoạt nhầm tập tin thực thi mà tập tin đó có thể là phần mềm có hại hoặc có chứa mã độc.

4. Các hành động sau đây phải được thông báo cho cán bộ chuyên trách công nghệ thông tin để được xem xét tư vấn và phải có sự đồng ý của thủ trưởng cơ quan trước khi tiến hành:

- Thay đổi cấu hình máy tính cá nhân do cơ quan cấp;

- Kết nối máy tính cá nhân do cơ quan cấp vào các mạng thông tin khác;

- Cài đặt các phần mềm khác với quy định của cơ quan lên máy tính cá nhân do cơ quan cấp;

- Kết nối máy tính thuộc sở hữu cá nhân vào hệ thống thông tin của cơ quan;

- Sử dụng máy tính cấp cho người sử dụng khác.

Điều 10. Đảm bảo an toàn thông tin số trong việc quản lý và sử dụng tài khoản

1. Mật khẩu của tất cả các tài khoản trong hệ thống thông tin của các cơ quan (ở cả cấp độ quản trị hệ thống và cấp độ người sử dụng) phải tuân thủ đồng thời các yêu cầu sau:

a) Có chứa cả các ký tự chữ in và chữ thường;

b) Có chứa ký tự số, các kí tự dấu câu hoặc các ký tự đặc biệt;

c) Có ít nhất 08 kí tự đối với tài khoản người dùng, ít nhất 15 ký tự đối với tài khoản quản trị hệ thống;

d) Không phải là một từ hoàn chỉnh trong các ngôn ngữ thông dụng (Tiếng Việt, Tiếng Anh, Tiếng Pháp,...);

đ) Không phải là một dãy ký tự lặp lại có quy luật;

e) Không dựa vào thông tin cá nhân (ngày sinh, số điện thoại,...), tên người, tên địa danh, tên cơ quan hoặc các tên gọi khác.

2. Các tài khoản quản trị hệ thống thông tin của cơ quan (bao gồm tài khoản đăng nhập để quản trị máy chủ, thiết bị mạng, ứng dụng và cơ sở dữ liệu trong hệ thống thông tin) phải được thay đổi mật khẩu định kỳ ít nhất ba (03) tháng một lần.

3. Tài khoản cấp cho người sử dụng để sử dụng các thành phần của hệ thống thông tin phải được thay đổi mật khẩu định kỳ ít nhất sáu (06) tháng một lần.

4. Các hành vi bị nghiêm cấm trong việc sử dụng tài khoản do cơ quan cấp:

a) Lưu trữ hoặc gửi mật khẩu các tài khoản trên phương tiện điện tử;

b) Dùng cùng một mật khẩu cho các tài khoản khác nhau để truy cập vào hệ thống thông tin của cơ quan;

c) Dùng mật khẩu trong hệ thống thông tin của cơ quan cho các tài khoản cá nhân;

d) Cho người khác biết mật khẩu (trừ trường hợp thủ trưởng cơ quan yêu cầu);

đ) Dùng chức năng ghi nhớ mật khẩu của các ứng dụng trên máy tính dùng chung;

e) Sử dụng mật khẩu đã bị đánh cắp hoặc nghi ngờ bị đánh cắp cho tài khoản cũ hoặc các tài khoản khác do cơ quan cấp;

g) Không kịp thời thông báo cho thủ trưởng cơ quan và cán bộ chuyên trách công nghệ thông tin biết khi nghi ngờ mật khẩu tài khoản của mình bị người khác biết ngoài ý muốn.

Điều 11. Phòng chống các phần mềm có hại (virus, worm, spyware...)

1. Các cơ quan phải triển khai các biện pháp phòng chống các phần mềm có hại đối với hệ thống thông tin của cơ quan theo quy định tại Điểm b Khoản 5 Điều 5 Quy định này; đồng thời thường xuyên tổ chức kiểm tra, rà soát đảm bảo người sử dụng phải sử dụng các chương trình chống phần mềm có hại do cơ quan cung cấp.

2. Những biện pháp phải thực hiện để phòng chống các phần mềm có hại đối với hệ thống thông tin của cơ quan:

a) Không tải dữ liệu từ những nguồn thông tin không rõ ràng hay nghi ngờ có hại cho máy tính cá nhân và hệ thống thông tin của cơ quan;

b) Không mở các tài liệu, tập tin gửi kèm trong các thư điện tử từ những địa chỉ không biết rõ hoặc không đáng tin cậy;

c) Không tự ý sử dụng tính năng chia quyền truy cập đĩa trực tiếp (disk sharing). Nếu do yêu cầu công việc cần sử dụng tính năng này thì phải được sự đồng ý của thủ trưởng cơ quan trước khi sử dụng;

d) Thực hiện kiểm tra virus và các phần mềm có hại khác trên các phương tiện lưu trữ gắn ngoài như USB, thẻ nhớ, đĩa cứng gắn ngoài,... trước khi sử dụng;

đ) Khi phát hiện có chương trình làm ảnh hưởng đến hoạt động của chương trình chống phần mềm có hại hoặc phần mềm ứng dụng của cơ quan, người sử dụng phải kịp thời báo cáo thủ trưởng cơ quan và cán bộ chuyên trách công nghệ thông tin để sớm có phương án xử lý.

Điều 12. Đảm bảo an toàn thông tin số trong việc sử dụng thư điện tử công vụ

1. Tài khoản Thư điện tử công vụ tỉnh Khánh Hòa cấp cho người sử dụng và các cơ quan sử dụng để phục vụ công việc. Việc quản lý, sử dụng thư điện tử công vụ phải tuân thủ quy định của Ủy ban nhân dân tỉnh và các quy định của pháp luật về quản lý, sử dụng thư điện tử.

2. Những biện pháp đảm bảo an toàn thông tin số trong việc sử dụng thư điện tử công vụ:

a) Thực hiện kiểm tra thông tin, dữ liệu đính kèm khi gửi/nhận/chuyển tiếp thư điện tử trên tài khoản thư điện tử công vụ để tránh việc tiết lộ thông tin nhạy cảm của cá nhân và cơ quan, tránh bị lợi dụng làm phương tiện phát tán thư rác và các phần mềm có hại;

b) Khi nhận được thư điện tử gửi kèm tập tin phải thực hiện quét virus và phần mềm độc hại cho tập tin trước khi mở hoặc chuyển cho người khác, kể cả trong các trường hợp không phát hiện dấu hiệu nghi ngờ;

c) Sử dụng chức năng đánh dấu thư rác (spam) để ngăn chặn các thư điện tử có dấu hiệu nghi ngờ, không rõ nguồn gốc hoặc thư rác;

d) Kịp thời thông báo cho cán bộ chuyên trách công nghệ thông tin hoặc báo cáo thủ trưởng cơ quan khi nhận được thư điện tử có dấu hiệu vi phạm pháp luật hoặc có khả năng gây ảnh hưởng đến công việc, uy tín, danh dự, tài sản của bản thân, cơ quan hoặc tổ chức, cá nhân khác để tiến hành các biện pháp kiểm tra, xử lý cần thiết;

đ) Không được thực hiện các hành vi sau đây:

- Sử dụng thư điện tử công vụ cho các mục đích mưu lợi cá nhân, phát tán các nội dung trái quy định của pháp luật hoặc không nhằm mục đích phục vụ cho công việc;

- Sử dụng thư điện tử công vụ nhằm quấy rối hay làm gián đoạn công việc của tổ chức, cá nhân khác;

- Truy cập tài khoản thư điện tử công vụ bằng máy tính hoặc từ mạng máy tính không đảm bảo an toàn thông tin số;

- Đặt chế độ chuyển thư tự động từ tài khoản thư điện tử công vụ được cấp tới tài khoản thư điện tử khác không phải do cơ quan nhà nước cấp;

- Gửi, nhận hoặc phát tán các phần mềm có hại, thư rác qua hệ thống thư điện tử công vụ.

3. Các cơ quan thường xuyên chủ động phối hợp với Sở Thông tin và Truyền thông tổ chức hướng dẫn cho người sử dụng của cơ quan các phương pháp phát hiện, xử lý thư điện tử có dấu hiệu nghi ngờ, không rõ nguồn gốc, thư điện tử giả mạo hoặc thư rác; đề nghị khóa hoặc thu hồi tài khoản thư điện tử công vụ nếu xét thấy việc sử dụng thư điện tử công vụ của người sử dụng không tuân thủ các quy định của pháp luật hoặc có khả năng làm tổn hại đến công việc, quan hệ và uy tín của cơ quan.

Điều 13. Đảm bảo an toàn thông tin số cho kết nối truy cập từ xa

1. Căn cứ hiện trạng và nhu cầu sử dụng hệ thống thông tin, các cơ quan có thể cho phép hoặc không cho phép thiết lập các kết nối từ xa vào hệ thống thông tin của cơ quan mình.

2. Việc kết nối từ xa vào hệ thống thông tin của các cơ quan phải đảm bảo các yêu cầu sau đây:

a) Xác định rõ mục đích, phương pháp, đối tượng sử dụng kết nối từ xa vào hệ thống thông tin của cơ quan;

b) Tuân thủ các tiêu chuẩn kỹ thuật để đảm bảo các kết nối từ xa vào hệ thống thông tin của cơ quan được giám sát chặt chẽ. Chỉ cho phép các thiết bị được trang bị cơ chế bảo mật (tối thiểu là cơ chế định danh thiết bị và trang bị phần mềm chống các phần mềm có hại) thực hiện kết nối từ xa vào hệ thống thông tin của cơ quan;

c) Đảm bảo việc quản lý, giám sát và sử dụng các kết nối từ xa vào hệ thống thông tin của cơ quan tuân thủ các quy định về đảm bảo an toàn thông tin số như các kết nối trực tiếp trong hệ thống thông tin của cơ quan;

3. Người sử dụng được cấp tài khoản để thực hiện kết nối từ xa vào hệ thống thông tin của cơ quan phải tuân thủ các quy định tại Điều 10 Quy định này và các quy định khác do thủ trưởng cơ quan ban hành.

Điều 14. Đảm bảo an toàn thông tin số cho cổng/trang thông tin điện tử

1. Các cơ quan phải xây dựng quy trình tạo lập, đăng tải, xử lý và hủy bỏ dữ liệu trên cổng/trang thông tin điện tử của cơ quan mình; đồng thời triển khai áp dụng các biện pháp giám sát các hoạt động này.

2. Cổng/trang thông tin điện tử của các cơ quan phải được áp dụng cơ chế sao lưu dữ liệu định kỳ (tối thiểu 01 lần/tuần) và lưu trữ nhật ký quản trị hệ thống phục vụ cho công tác quản lý và khắc phục các sự cố có thể xảy ra.

3. Khi cung cấp các dịch vụ cần phải định danh người sử dụng, cổng/trang thông tin điện tử của các cơ quan phải có cơ chế xác thực, cấp phép truy cập, mã hóa thông tin, dữ liệu cho việc truy cập vào các dịch vụ đó. Việc cấp, quản lý và sử dụng tài khoản đăng nhập vào cổng/trang thông tin điện tử phải tuân thủ các quy định tại Điều 10 Quy định này.

4. Cổng/trang thông tin điện tử có thực hiện việc thu thập, sử dụng thông tin cá nhân của người sử dụng phải xây dựng và áp dụng quy trình cụ thể trong việc thu thập, sử dụng và chia sẻ thông tin cá nhân; đồng thời phải thông báo trên trang chủ của cổng/trang thông tin điện tử cho người sử dụng biết về chính sách bảo đảm an toàn thông tin cá nhân.

Chương IV
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN SỐ

Điều 15. Trách nhiệm của thủ trưởng cơ quan

1. Tổ chức thực hiện nghiêm túc các nội dung của Quy định này, chịu trách nhiệm trước Tỉnh ủy, Ủy ban nhân dân tỉnh và cơ quan cấp trên trực tiếp về công tác đảm bảo an toàn thông tin số cho hệ thống thông tin của cơ quan.

2. Ban hành quy định quản lý, vận hành, khai thác, sử dụng hệ thống thông tin của cơ quan (trong đó bao gồm các quy định và quy trình đảm bảo an toàn thông tin số) theo quy định tại Điều 7 Quy định này và hướng dẫn của Sở Thông tin và Truyền thông.

3. Thường xuyên quan tâm đầu tư, nâng cấp, bảo dưỡng thiết bị, đào tạo người sử dụng để tăng cường công tác đảm bảo an toàn thông tin số.

4. Phổ biến, quán triệt các nội dung của Quy định này đến từng cán bộ, công chức, người lao động; tổ chức trang bị các kiến thức bảo mật cơ bản cho người sử dụng của cơ quan theo hướng dẫn của Sở Thông tin và Truyền thông.

5. Bố trí cán bộ chuyên trách công nghệ thông tin để tham mưu, triển khai công tác đảm bảo an toàn thông tin số; tạo điều kiện để cán bộ chuyên trách công nghệ thông tin được đảm bảo điều kiện học tập, tiếp thu công nghệ, kiến thức về an toàn, bảo mật thông tin.

6. Khi có sự cố hoặc nguy cơ mất an toàn thông tin số, kịp thời áp dụng mọi biện pháp để khắc phục và hạn chế thiệt hại; ưu tiên sử dụng lực lượng kỹ thuật an toàn thông tin số của đơn vị; lập biên bản, báo cáo bằng văn bản cho cơ quan cấp trên quản lý trực tiếp. Trường hợp có sự cố nghiêm trọng vượt quá khả năng khắc phục của cơ quan, phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và thông báo Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ.

7. Tạo điều kiện cho các cơ quan chức năng tham gia khắc phục sự cố gây mất an toàn thông tin số.

8. Phối hợp với sở Thông tin và Truyền thông trong công tác kiểm tra việc thực hiện Quy định này.

9. Báo cáo tình hình và kết quả thực hiện công tác đảm bảo an toàn thông tin số của cơ quan, gửi về Sở Thông tin và Truyền thông trước ngày 30 tháng 11 hàng năm.

Điều 16. Trách nhiệm của cán bộ chuyên trách công nghệ thông tin

1. Chịu trách nhiệm triển khai các biện pháp quản lý vận hành, quản lý kỹ thuật và tham mưu xây dựng các quy định và quy trình nội bộ đảm bảo an toàn thông tin số cho hệ thống thông tin của cơ quan.

2. Tham mưu thủ trưởng cơ quan tổ chức thực hiện các biện pháp quản lý chuyên môn và vận hành an toàn hệ thống thông tin của cơ quan theo nội dung của Quy định này.

3. Phối hợp với các cá nhân, cơ quan liên quan trong việc kiểm tra, phát hiện và khắc phục sự cố gây mất an toàn thông tin số.

4. Tham gia các chương trình đào tạo, hội nghị về công tác đảm bảo an toàn thông tin số do Sở Thông tin và Truyền thông và các cơ quan liên quan tổ chức.

Điều 17. Trách nhiệm của người sử dụng

1. Nâng cao ý thức cảnh giác, trách nhiệm đảm bảo an toàn thông tin số, thực hiện nghiêm các nội dung Quy định này, các quy định về an toàn thông tin số của cơ quan đang công tác và các quy định của pháp luật trong việc khai thác, sử dụng các thành phần trong hệ thống thông tin của cơ quan.

2. Khi phát hiện sự cố gây mất an toàn thông tin số, phải báo cáo ngay với cấp trên và cán bộ chuyên trách công nghệ thông tin để kịp thời ngăn chặn, xử lý.

3. Hưởng ứng, tham gia các chương trình đào tạo, hội nghị về an toàn thông tin số do Sở Thông tin và Truyền thông và các cơ quan liên quan tổ chức.

Điều 18. Trách nhiệm của Sở Thông tin và Truyền thông

1. Tham mưu Ủy ban nhân dân tỉnh về công tác đảm bảo an toàn thông tin số trên địa bàn tỉnh và chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong việc đảm bảo an toàn thông tin số cho Mạng diện rộng (WAN) của tỉnh, Trung tâm dữ liệu và các hệ thống thông tin đặt tại Trung tâm dữ liệu của tỉnh.

2. Xây dựng nội dung, tổ chức hướng dẫn và triển khai thực hiện các chương trình đào tạo, hội nghị tuyên truyền đảm bảo an toàn thông tin số trong công tác quản lý nhà nước trên địa bàn tỉnh.

3. Tham mưu thành lập Đội ứng cứu sự cố máy tính trên địa bàn tỉnh trực thuộc Ủy ban nhân dân tỉnh. Tổ chức và thực hiện chức năng đầu mối mạng lưới ứng cứu sự cố máy tính trên địa bàn tỉnh theo sự điều phối của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT). Phối hợp VNCERT và các đơn vị liên quan để hướng dẫn xử lý, ứng cứu các sự cố gây mất an toàn thông tin số trên địa bàn tỉnh.

Hàng năm xây dựng kế hoạch đào tạo nâng cao trình độ nghiệp vụ chuyên môn về an toàn, an ninh thông tin cho Đội ứng cứu sự cố máy tính và đội ngũ cán bộ chuyên trách công nghệ thông tin của các cơ quan.

4. Hướng dẫn các cơ quan xây dựng và ban hành các quy định và quy trình đảm bảo an toàn thông tin số theo quy định tại Điều 7 Quy định này.

5. Hướng dẫn các cơ quan trong việc đầu tư trang thiết bị và các ứng dụng phục vụ công tác đảm bảo an toàn thông tin số cho hệ thống thông tin của các cơ quan, phù hợp với hệ thống thông tin của tỉnh.

6. Hướng dẫn các cơ quan thực hiện các báo cáo về sự cố mất an toàn thông tin số và kết quả thực hiện công tác đảm bảo an toàn thông tin số tại các cơ quan.

7. Tổng hợp tình hình và kết quả thực hiện công tác đảm bảo an toàn thông tin số trên địa bàn tỉnh, định kỳ báo cáo Tỉnh ủy, Ủy ban nhân dân tỉnh, Bộ Thông tin và Truyền thông trước ngày 30 tháng 12 hàng năm.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 19. Kiểm tra, đánh giá công tác đảm bảo an toàn thông tin số

1. Sở Thông tin và Truyền thông chủ trì, phối hợp với các cơ quan có liên quan lập kế hoạch và tiến hành kiểm tra công tác đảm bảo an toàn thông tin số định kỳ hàng năm hoặc đột xuất khi phát hiện có dấu hiệu vi phạm công tác đảm bảo an toàn thông tin số trong hệ thống thông tin của các cơ quan. Việc kiểm tra công tác đảm bảo an toàn thông tin số định kỳ hàng năm có thể được tiến hành lồng ghép trong kế hoạch kiểm tra các nội dung liên quan đến công tác đánh giá mức độ ứng dụng công nghệ thông tin trong hoạt động của các cơ quan.

2. Văn phòng Ủy ban nhân dân tỉnh, Sở Nội vụ, Công an tỉnh và các cơ quan liên quan có trách nhiệm phối hợp với Sở Thông tin và Truyền thông trong việc xây dựng kế hoạch, tổ chức thực hiện công tác kiểm tra và xử lý vi phạm theo quy định của pháp luật.

3. Sở Thông tin và Truyền thông chủ trì, phối hợp với các cơ quan liên quan tổ chức đánh giá, xếp hạng công tác đảm bảo an toàn thông tin số của các cơ quan nhà nước trên địa bàn tỉnh theo quy định; đồng thời tham mưu mở rộng đối tượng đánh giá, xếp hạng đến các cơ quan Đảng, Mặt trận Tổ quốc và các tổ chức đoàn thể chính trị - xã hội thuộc tỉnh.

Điều 20. Tổ chức thực hiện

1. Hàng năm, Sở Thông tin và Truyền thông căn cứ số liệu báo cáo, kết quả kiểm tra và bảng xếp hạng an toàn thông tin số của các cơ quan để đề xuất Ủy ban nhân dân tỉnh xét khen thưởng các cá nhân, đơn vị theo quy định hiện hành.

2. Tổ chức, cá nhân có hành vi vi phạm các nội dung của Quy định này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật theo trách nhiệm, xử phạt hành

chính hoặc bị truy cứu trách nhiệm hình sự, nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật.

3. Trong quá trình thực hiện, nếu phát sinh khó khăn, vướng mắc hoặc cần sửa đổi, bổ sung, các cơ quan kịp thời phản ánh về Sở Thông tin và Truyền thông để tổng hợp, trình Ủy ban nhân dân tỉnh xem xét, quyết định./.

TM. ỦY BAN NHÂN DÂN

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Nguyễn Duy Bắc