UỶ BAN NHÂN DÂN **TỈNH ĐẮK LẮK**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 20/2016/QĐ-UBND	*Đắk Lắk, ngày 17 tháng 5 năm 2016*

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Đắk Lắk

ỦY BAN NHÂN DÂN TỈNH

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

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 18/TTr-STTTT ngày 15 tháng 3 năm 2016,

QUYẾT ĐỊNH:

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

Điều 2. Giao Sở Thông tin và Truyền thông chủ trì, phối hợp các Sở, ban, ngành có liên quan; Ủy ban nhân dân các huyện, thị xã, thành phố triển khai, thực hiện Quyết định này.

Điều 3. Quyết định này có hiệu lực kể từ ngày 27 tháng 5 năm 2016.

Chánh Văn phòng Ủy ban nhân dân tỉnh; Giám đốc các Sở, ban, ngành ở tỉnh; Chủ tịch Ủy ban nhân dân các huyện, thị xã, thành phố; Thủ trưởng các đơn vị, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Phạm Ngọc Nghị

UỶ BAN NHÂN DÂN
TỈNH ĐẮK LẮK

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

QUY CHẾ
Bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Đắk Lắk

(Ban hành kèm theo Quyết định số 20/2016/QĐ-UBND ngày 17 tháng 5 năm 2016 của Ủy ban nhân dân tỉnh Đắk Lắk)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về công tác để bảo đảm an toàn, an ninh thông tin bao gồm: nguyên tắc bảo đảm an toàn, an ninh thông tin; bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin, an toàn thông tin trên môi trường mạng; bảo vệ thông tin cá nhân trên môi trường mạng; quản lý nhà nước về an toàn thông tin; quyền và nghĩa vụ của cơ quan, đơn vị, tổ chức, cá nhân và doanh nghiệp có tham gia hoạt động phát triển, ứng dụng công nghệ thông tin trên địa bàn tỉnh Đắk Lắk.

Điều 2. Đối tượng áp dụng

Quy chế này được áp dụng đối với các cơ quan, đơn vị, doanh nghiệp, tổ chức, cá nhân có tham gia phát triển và ứng dụng công nghệ thông tin trên địa bàn tỉnh Đắk Lắk.

Điều 3. Giải thích từ ngữ

1. *An toàn thông tin:* Là sự bảo vệ thông tin và hệ thống thông tin tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

2. *An ninh thông tin:* Là sự bảo đảm thông tin, hệ thống thông tin được phục vụ liên tục, tránh bị gián đoạn, ngăn chặn các truy nhập trái phép làm sửa đổi, phá hoại hoặc rò rỉ thông tin.

3. *Hệ thống thông tin:* Là tập hợp thiết bị phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin.

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

5. *Xâm phạm an toàn thông tin:* Là hành vi truy nhập, sử dụng, sửa đổi, tiết lộ thông tin trái phép; làm gián đoạn, làm sai lệch chức năng, phá hoại trái phép thông tin và hệ thống thông tin.

6. *Tập tin vết (Log File):* Là một tập tin được tạo ra bởi một máy chủ web hoặc máy chủ proxy có chứa tất cả thông tin về các hoạt động trên máy chủ đó.

7. *Tường lửa (Firewall):* 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.

8. *Môi trường mạng:* Là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua cơ sở hạ tầng thông tin.

9. *Máy chủ:* Là máy có cấu hình cao, được cài đặt hệ điều hành riêng cho máy dùng để làm trung tâm kết nối các máy tính trong một văn phòng, công ty, cơ quan lại với nhau... và nó là nơi trao đổi dữ liệu, điều hành chung của mạng máy tính, dùng làm server cho web, webmail...

10. *Máy trạm:* Là máy tính dùng cho cá nhân sử dụng, chủ yếu phục vụ nhu cầu làm việc, học hành, vui chơi, giải trí…

11. *Cán bộ chuyên trách công nghệ thông tin của cơ quan nhà nước:* là công chức có chuyên môn nghiệp vụ về công nghệ thông tin đã được tuyển dụng và đang làm nhiệm vụ quản lý nhà nước chuyên ngành công nghệ thông tin; viên chức có chuyên môn về công nghệ thông tin đã được tuyển dụng và đang làm công tác quản lý, phát triển, vận hành hệ thống công nghệ thông tin tại các đơn vị sự nghiệp thuộc Sở Thông tin và Truyền thông; công chức đảm bảo tiêu chuẩn chuyên môn, nghiệp vụ công nghệ thông tin đã được tuyển dụng và đang thực hiện công tác quản lý, vận hành, phát triển hệ thống công nghệ thông tin tại các Sở, ban, ngành, Ủy ban nhân dân các huyện, thị xã, thành phố.

12. *Bí mật nhà nước:* là những tin về vụ, việc, tài liệu, vật, địa điểm, thời gian, lời nói có nội dung quan trọng thuộc lĩnh vực chính trị, quốc phòng, an ninh, đối ngoại, kinh tế, khoa học, công nghệ, các lĩnh vực khác mà Nhà nước không công bố hoặc chưa công bố và nếu tiết lộ thì gây nguy hại cho nước Cộng hòa Xã hội Chủ nghĩa Việt Nam.

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

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

Điều 4. Nguyên tắc bảo đảm an toàn, an ninh thông tin

1. Tổ chức, cá nhân có trách nhiệm bảo đảm an toàn, an ninh thông tin trong mọi hoạt động ứng dụng công nghệ thông tin của đơn vị mình. Hoạt động an toàn thông tin của tổ chức, cá nhân phải phù hợp với quy định của Luật An toàn thông tin mạng, Luật Công nghệ thông tin và các quy định pháp luật khác có liên quan đến việc đảm bảo an toàn thông tin.

2. Tổ chức, cá nhân không được xâm phạm an toàn, an ninh thông tin của tổ chức, cá nhân khác.

3. Tổ chức, cá nhân tham gia hoạt động an toàn thông tin có trách nhiệm phối hợp với cơ quan quản lý nhà nước có thẩm quyền và với tổ chức, cá nhân khác trong việc bảo đảm an toàn, an ninh thông tin.

4. Xử lý sự cố thông tin phải đảm bảo quyền và lợi ích hợp pháp của tổ chức, cá nhân; không xâm phạm đến bí mật đời tư của cá nhân, thông tin riêng của tổ chức, cá nhân.

5. Hoạt động bảo đảm an toàn, an ninh thông tin phải được thực hiện thường xuyên, liên tục và hiệu quả trên cơ sở tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin.

6. Các hoạt động ứng dụng công nghệ thông tin trong cơ quan nhà nước phải tuân theo nguyên tắc bảo đảm an toàn thông tin được quy định tại Điều 41, Nghị định

64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước và quy định tại Quy chế này.

Chương II
CÔNG TÁC BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN

Điều 5. Điều kiện bảo đảm 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, doanh nghiệp bố trí cán bộ làm công tác chuyên trách hoặc phụ trách công nghệ thông tin phải có chuyên ngành phù hợp và được đào tạo, bồi dưỡng kịp thời về chuyên môn đối với lĩnh vực an toàn, an ninh thông tin.

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

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

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

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

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

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

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

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

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

h) Tổ chức thực hiện.

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

1. Phòng máy chủ tại các Trung tâm dữ liệu:

a) Phòng máy chủ được thiết kế, xây dựng, vận hành và khai thác phải áp dụng tiêu chuẩn, quy chuẩn kỹ thuật tại thông tư 03/2013/TT-BTTTT ngày 22 tháng 01 năm 2013 về việc quy định áp dụng tiêu chuẩn, quy chuẩn kỹ thuật đối với trung tâm dữ liệu của Bộ Thông tin và Truyền thông.

b) Các thiết bị mạng quan trọng như tường lửa, thiết bị định tuyến, hệ thống máy chủ, … phải được đặt trong phòng máy chủ và có các biện pháp bảo vệ, ngăn chặn xâm nhập trái phép vào phòng máy chủ; là khu vực hạn chế tiếp cận và được lắp đặt hệ thống camera giám sát. Phòng máy chủ phải có hệ thống máy phát điện, hệ

thống lưu điện đủ công suất để bảo đảm duy trì hệ thống thiết bị và máy chủ hoạt động liên tục theo yêu cầu kỹ thuật.

c) Chỉ những người có trách nhiệm theo quy định của Thủ trưởng cơ quan mới được phép vào phòng máy chủ. Quá trình vào, ra phòng máy chủ phải được ghi nhận vào nhật ký quản lý phòng máy chủ.

d) Bố trí cán bộ có năng lực chuyên môn cao để quản lý, vận hành phòng máy chủ và duy trì chế độ trực 24/7 để hệ thống hoạt động liên tục và bảo đảm công tác an toàn thông tin mạng.

2. Máy chủ:

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

3. Thiết bị chống sét, phòng cháy, chữa cháy:

Các cơ quan, doanh nghiệp phải lắp đặt thiết bị chống sét, trang bị thiết bị phòng cháy, chữa cháy để bảo vệ các hệ thống công nghệ thông tin an toàn.

4. Thiết bị chuyển mạch (Router/Switch):

Thiết bị chuyển mạch mạng tin học của các cơ quan, doanh nghiệp phải bảo đảm khả năng cung cấp các chức năng quản trị nhằm tăng cường độ an toàn và bảo mật cho hệ thống mạng, như: Cung cấp khả năng từ chối các kết nối không mong muốn hay trái phép vào hệ thống và khống chế số lượng kết nối vào hệ thống mạng nội bộ thông qua thiết bị chuyển mạch. Phải có ít nhất 01 thiết bị chuyển mạch hỗ trợ định tuyến IP cho mỗi mạng nội bộ, hỗ trợ chức năng điều khiển truy cập, chức năng xác thực thiết bị, xác thực người sử dụng và chức năng bảo mật quản trị mạng.

5. Tường lửa:

Phòng máy chủ phải xây dựng tường lửa bảo đảm các yêu cầu, khả năng xử lý được số lượng kết nối đồng thời cao và chịu được băng thông cao, hỗ trợ các công nghệ mạng riêng ảo thông dụng; có phần cứng mã hoá tích hợp để tăng khả năng mã hoá dữ liệu, cung cấp đầy đủ các cơ chế bảo mật cơ bản, quản lý luồng dữ liệu ra, vào và có khả năng giảm thiểu rủi ro cho hệ thống trước các loại tấn công từ chối dịch vụ.

6. Hệ thống lưu trữ:

Năng lực I/O (nhập xuất) phải đáp ứng đầy đủ các yêu cầu truy xuất dữ liệu và dung lượng lưu trữ của các ứng dụng và dịch vụ đang hoạt động trên hệ thống công nghệ thông tin của cơ quan, đơn vị; độ bền và độ ổn định phải cao, bảo đảm hoạt động liên tục trong thời gian dài, không gây gián đoạn.

7. Trong quá trình đầu tư mua sắm trang thiết bị công nghệ thông tin phải đảm bảo chất lượng máy móc, thiết bị, phần mềm và cần lưu ý đến xuất xứ hàng hóa để bảo đảm an toàn, an ninh thông tin mạng.

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

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

1. Quản lý tài nguyên: Cán bộ quản trị mạng có trách nhiệm kiểm tra, giám sát chức năng chia sẻ thông tin; tổ chức cấp phát tài nguyên trên máy chủ theo danh mục

thư mục cho từng đơn vị, tổ chức, phòng, ban…; khuyến cáo người dùng cân nhắc việc chia sẻ tài nguyên cục bộ trên máy đang sử dụng, tuyệt đối không được chia sẻ toàn bộ ổ cứng. Khi thực hiện chia sẻ tài nguyên trên máy chủ hoặc trên máy cục bộ phải sử dụng mật khẩu để bảo vệ thông tin.

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

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

4. Quản lý nhật ký: Hệ thống 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 tập tin vết theo từng tháng để lưu vết theo dõi, xác định những sự kiện đã xảy ra của hệ thống và hạn chế việc tràn tập tin vết gây ảnh ưởng đến hoạt động của hệ thống.

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

6. Quản lý cài đặt: Người sử dụng khi cài đặt thêm chương trình khác trên máy tính cá nhân được cơ quan nhà nước, tổ chức, doanh nghiệp trang bị trong quá trình làm việc phải có xuất xứ nguồn gốc rõ ràng, tin cậy nhằm tránh sự lây lan của virus. Cán bộ chuyên trách công nghệ thông tin có trách nhiệm kiểm tra về mức độ an toàn, bảo mật các phần mềm ứng dụng phục vụ công tác chuyên ngành tại các máy tính của người sử dụng.

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

Điều 8. Bảo vệ bí mật nhà nước trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước

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 mật, chuyển giao, lưu trữ thông tin có nội dung thuộc bí mật nhà nước; không được cung cấp tin, tài liệu và đưa thông tin bí mật nhà nước trên hệ thống cổng/trang thông tin điện tử và truyền tải trên môi trường mạng.

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, người có trách nhiệm, cấp có thẩm quyền (nếu cần) để thực hiện các biện pháp sao lưu, bảo mật thông tin, dữ liệu trước khi sửa chữa. Không được cho phép cá nhân không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố trên các máy tính có chứa thông tin, tài liệu mật.

3. Trước khi thanh lý các máy tính trong các cơ quan nhà nước, cán bộ chuyên trách công nghệ thông tin phải dùng các biện pháp kỹ thuật xoá bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

Điều 9. Quản lý, vận hành hệ thống thông tin của cơ quan, đơn vị, tổ chức, doanh nghiệp

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

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

3. Hệ thống thông tin của cơ quan, 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 tập tin vết ra, vào hệ thống để phục vụ công tác khắc phục sự cố, điều tra, phân tích và làm rõ các nguy cơ gây mất an toàn, an ninh thông tin; chức năng ngăn chặn người dùng truy cập thông tin trái với các quy định Pháp luật.

4. Hệ thống mạng không dây (wireless) của các cơ quan, đơn vị phải được sử dụng tiêu chuẩn bảo mật mạng không dây với độ dài khoá tối thiểu 128 bit, đồng thời phải thiết lập khoá khi truy cập tối thiểu 8 ký tự, có những kí tự chữ và số, khuyến cáo nên có ký tự đặc biệt.

5. Mạng riêng ảo (VPN) của các cơ quan, đơn vị kết nối để truy cập vào hệ thống thông tin phải được bảo mật, quản lý và kiểm soát chặt chẽ các kết nối; hủy bỏ kết nối khi không còn sử dụng. Bảo đảm chỉ có cán bộ, nhân viên được cấp phép mới có quyền truy cập vào mạng nội bộ thông qua VPN.

6. Hệ thống quản trị mạng tập trung (Network Management System) của cơ quan, đơn vị nhằm theo dõi hoạt động của các thiết bị, dịch vụ và phần mềm trong hệ thống thông tin. Phối hợp với các hệ thống an toàn bảo mật khác để đánh giá và phân tích năng lực hoạt động của toàn bộ hệ thống thông tin, từ đó đưa ra các biện pháp vận hành hợp lý bảo đảm sự ổn định, sẵn sàng của hệ thống.

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

8. Khi cơ quan, đơn vị, tổ chức, doanh nghiệp có cán bộ chuyển công tác, thay đổi vị trí việc làm hoặc nghỉ hưu, nghỉ việc phải có biện pháp thay đổi hoặc huỷ bỏ tài khoản đang sử dụng hiện tại trên hệ thống.

Điều 10. Quản trị cổng/trang thông tin điện tử của cơ quan, đơn vị

1. Đối với biên tập viên đăng tải thông tin:

Biên tập viên khi đăng nhập vào phần quản trị để đăng tải thông tin phải sử dụng máy tính được cơ quan, đơn vị trang bị có phần mềm diệt vi rút bản quyền, không dùng máy tính công cộng. Kết nối internet phải là kết nối từ mạng của cơ quan hoặc nhà riêng, không dùng kết nối những nơi công cộng như quán cà phê, điểm truy cập internet công cộng…; tuyệt đối không được đăng, tải liên kết thông tin không rõ nguồn gốc xuất xứ hoặc chưa được sự cho phép của chủ sở hữu thông tin. Biên tập viên định kỳ 06 tháng 01 lần phải thay đổi mật khẩu của mình. Khi đã thực hiện xong việc đăng, tải thông tin, biên tập viên phải đăng xuất ra khỏi tài khoản của mình đúng quy trình kỹ thuật sử dụng hệ thống.

2. Đối với quản trị viên hệ thống:

Quản trị viên đăng nhập vào phần quản trị phải sử dụng máy tính cá nhân được cơ quan cấp trong quá trình làm việc, có phần mềm diệt vi rút bản quyền. Kết nối internet phải là kết nối từ mạng của cơ quan hoặc nhà riêng, không dùng kết nối những nơi công cộng như quán cà phê, điểm truy cập internet công cộng…Quản trị viên định kỳ 03 tháng 01 lần thay đổi mật khẩu của mình. Khi có sự cố tấn công về cổng/trang thông tin điện tử, quản trị viên thông báo ngay với thủ trưởng cơ quan quản lý và Sở Thông tin và Truyền thông để phối hợp với Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam cùng xử lý. Đồng thời liên hệ với nơi cung cấp dịch lưu trữ (hosting) tạm thời ngắt kết nối, đợi xử lý xong sự cố mới cho cổng/trang thông tin điện tử hoạt động trở lại.

Điều 11. Quyền hạn, nhiệm vụ của cán bộ chuyên trách công nghệ thông tin hoặc cán bộ, nhân viên phụ trách công nghệ thông tin của cơ quan, đơn vị, tổ chức, doanh nghiệp

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

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

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

4. Triển khai áp dụng các giải pháp tổng thể bảo đảm an toàn, an ninh thông tin mạng trong toàn hệ thống; thực hiện 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 bảo đảm tính sẵn sàng, tin cậy và toàn vẹn.

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

Điều 12. Giải quyết và khắc phục sự cố an toàn, an ninh thông tin

1. Đối với người sử dụng:

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

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

2. Đối với các cơ quan, đơn vị, tổ chức, doanh nghiệp chỉ đạo cán bộ chuyên trách, phụ trách công nghệ thông tin thực hiện một số thao tác cơ bản như sau:

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

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

Bước 2: Sao chép nhật ký tập tin vết 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.

Bước 4: Lập biên bản ghi nhận sự cố gây ra mất an toàn, an ninh thông tin đối với hệ thống thông tin của cơ quan, đơn vị; đồng thời thu thập các chứng cứ, dấu vết và nguyên nhân gây ra sự cố (nếu có); báo cáo sự cố và kết quả khắc phục sự cố cho Thủ trưởng cơ quan, đơn vị.

b) Trong trường hợp phát hiện sự cố xảy ra ngoài khả năng giải quyết của cơ quan, đơn vị phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông để được hỗ trợ, hướng dẫn, khắc phục sự cố; trong trường hợp cần thiết phải báo cáo sự cố kịp thời cho Công an tỉnh để cùng phối hợp xử lý.

3. Sở Thông tin và Truyền thông:

a) Quyết định toàn diện về mặt kỹ thuật, công tác phối hợp trong quá trình khắc phục sự cố về an toàn, an ninh thông tin.

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

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

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

đ) Trong trường hợp sự cố xảy ra có phạm vi rộng, ảnh hưởng và liên quan đến nhiều ngành, nhiều lĩnh vực phải thông báo khẩn cấp và xin ý kiến chỉ đạo của Ủy ban nhân dân tỉnh, Bộ Thông tin và Truyền thông.

Điều 13. Các doanh nghiệp phát triển, kinh doanh dịch vụ ứng dụng công nghệ thông tin

1. Các doanh nghiệp phát triển, kinh doanh dịch vụ ứng dụng công nghệ thông tin cho tổ chức, cá nhân phải đảm bảo các điều kiện về tiêu chuẩn kỷ thuật, cơ sở hạ tầng; thực hiện đầy đủ các quy định về công tác bảo đảm an toàn, an ninh thông tin theo quy định Pháp luật và có trách nhiệm báo cáo phối hợp với cơ quan quản lý nhà nước để khắc phục sự cố, xử lý vi phạm về công tác an toàn, an ninh thông tin.

2. Các doanh nghiệp cung cấp sản phẩm công nghệ thông tin phải cung cấp sản phẩm có nguồn gốc xuất xứ rõ ràng và đã qua kiểm định, kiểm soát hàng hoá của cơ

quan quản lý nhà nước theo quy định Pháp luật. Tuyệt đối không được cài đặt phần mềm bẻ khoá, phần mềm bản quyền không hợp pháp và không bản quyền lên thiết bị công nghệ thông tin để lưu thông ra thị trường.

3. Các doanh nghiệp cho thuê dịch vụ công nghệ thông tin phải bảo đảm an toàn, an ninh thông tin của các tổ chức, cá nhân sử dụng dịch vụ.

Chương III
TRÁCH NHIỆM VỀ CÔNG TÁC BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN

Điều 14. Trách nhiệm của Sở Thông tin và Truyền thông

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

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

a) Văn bản chỉ đạo, kế hoạch, đề án nhằm bảo đảm công tác an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin.

b) Xây dựng tiêu chuẩn đánh giá mức độ an toàn, an ninh thông tin đối với hệ thống thông tin của các cơ quan, đơn vị, tổ chức, doanh nghiệp khi tham gia hoạt động phát triển và ứng dụng công nghệ thông tin.

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

3. Hàng năm, tổ chức tập huấn, bồi dưỡng cán bộ chuyên trách, phụ trách công nghệ thông tin trên địa bàn tỉnh nhằm đào tạo chuyên sâu về công tác an toàn, an ninh thông tin cho lực lượng bảo đảm an toàn, an ninh thông tin mạng của các cơ quan, đơn vị; diễn tập về công tác an toàn, an ninh thông tin; tổ chức Hội nghị, Hội thảo chuyên đề về an toàn, an ninh thông tin.

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

5. Phối hợp với Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) và các đơn vị có liên quan trong thực hiện nhiệm vụ bảo đảm an toàn, an ninh thông tin mạng.

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

7. Tổng hợp báo cáo và thông báo về tình hình an toàn, an ninh thông tin mạng theo định kỳ cho Bộ Thông tin và Truyền thông, Ủy ban nhân dân tỉnh theo quy định.

8. Tăng cường công tác tuyên truyền, phổ biến pháp luật về an toàn, an ninh thông tin.

Điều 15. Trách nhiệm của Công an tỉnh

1. Chủ trì, phối hợp với Sở Thông tin và Truyền thông và các cơ quan, đơn vị có liên quan để xử lý, kiểm soát, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống thông tin gây phương hại đến an toàn, an ninh thông tin mạng.

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

3. Thực hiện nhiệm vụ bảo vệ an toàn các công trình, mạng lưới về an ninh quốc gia trên lĩnh vực công nghệ thông tin.

Điều 16. Trách nhiệm của các cơ quan, đơn vị, tổ chức, doanh nghiệp

1. Thủ trưởng các cơ quan, đơn vị, tổ chức, doanh nghiệp chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong công tác bảo đảm an toàn, an ninh thông tin đối với toàn bộ hệ thống thông tin của đơn vị mình, bao gồm các đơn vị trực thuộc. Thực hiện các trách nhiệm quy định tại Khoản 2 Điều 17, đồng thời chỉ đạo cán bộ chuyên trách, phụ trách công nghệ thông tin thực hiện nội dung quy chế, tham gia các hoạt động khắc phục sự cố.

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

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

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

5. Tạo điều kiện thuận lợi cho các cơ quan chức năng trong công tác điều tra, làm rõ nguyên nhân gây ra sự cố, khắc phục sự cố theo hướng dẫn chuyên môn của Sở Thông tin và Truyền thông.

Điều 17. Trách nhiệm của cán bộ, công chức, viên chức tại các cơ quan, đơn vị, tổ chức, doanh nghiệp

1. Trách nhiệm của cán bộ chuyên trách, 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 bảo đảm an toàn, an ninh thông tin 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 an toàn, an ninh thông tin.

c) Tuân thủ theo sự hướng dẫn kỹ thuật của Sở Thông tin và Truyền thông trong quá trình khắc phục sự cố về an toàn, an ninh thông tin.

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

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

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

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

Điều 18. Trách nhiệm của các tổ chức, doanh nghiệp cung cấp hạ tầng mạng và dịch vụ Internet, dịch vụ ứng dụng CNTT.

1. Phải thiết lập hệ thống trang thiết bị kỹ thuật, tổ chức và duy trì hoạt động phù hợp với quy mô cung cấp dịch vụ; đội ngũ nhân viên kỹ thuật, nhân viên quản lý điều hành đáp ứng được yêu cầu chuyên môn về an toàn thông tin; hệ thống thiết bị kỹ thuật đảm bảo phù hợp với quy định của pháp luật; phương án kỹ thuật khả thi, phù hợp tiêu chuẩn, quy chuẩn kỹ thuật; phương án kinh doanh khả thi phù hợp với quy định của pháp luật; phương án bảo mật thông tin khách hàng trong quá trình cung cấp dịch vụ trước và sau khi kết thúc hợp đồng cung cấp dịch vụ.

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

Chương IV
KIỂM TRA CÔNG TÁC BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN

Điều 19. Trách nhiệm và phối hợp trong công tác kiểm tra

1. Sở Thông tin và Truyền thông chủ trì, phối hợp với Công an tỉnh và các đơn vị có liên quan tiến hành kiểm tra định kỳ hàng năm đối với công tác bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin các tổ chức, cá nhân trên địa bàn tỉnh.

2. Công an tỉnh cử cán bộ phối hợp, tham gia đoàn kiểm tra, đánh giá công tác bảo đảm an toàn, an ninh thông tin các tổ chức, cá nhân; điều tra và xử lý các trường hợp vi phạm các quy định về an toàn, an ninh thông tin theo thẩm quyền.

3. Các cơ quan liên quan được mời tham gia đoàn kiểm tra: Cử cán bộ có chuyên môn về công nghệ thông tin tham gia đoàn kiểm tra do Sở Thông tin và Truyền thông tổ chức; phối hợp với đoàn kiểm tra xây dựng các tiêu chí và quy trình kỹ thuật kiểm tra công tác bảo đảm an toàn, an ninh thông tin.

4. Sở Thông tin và Truyền thông, Công an tỉnh có thẩm quyền tiến hành kiểm tra các tổ chức, cá nhân khi phát hiện có dấu hiệu vi phạm pháp luật về an toàn, an ninh thông tin.

5. Đoàn kiểm tra có trách nhiệm thông báo thời gian, địa điểm, nội dung và thành phần cho các tổ chức, cá nhân được kiểm tra biết trước ít nhất 05 ngày nếu kiểm tra định kỳ, ít nhất 01 giờ nếu kiểm tra đột xuất.

6. Tổ chức, cá nhân được kiểm tra:

a) Chuẩn bị nội dung báo cáo theo yêu cầu của Đoàn kiểm tra.

b) Có đại diện lãnh đạo và cán bộ liên quan của đơn vị để cùng làm việc với Đoàn kiểm tra.

c) Tạo thuận lợi cho công tác kiểm tra.

Điều 20. Kiểm tra định kỳ và đột xuất

1. Cơ quan chuyên trách về công tác an toàn thông tin của tỉnh (Sở Thông tin và Truyền thông) xây dựng kế hoạch và thực hiện công tác phối hợp kiểm tra định kỳ

hàng năm về công tác bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước, tổ chức, doanh nghiệp liên quan trên địa bàn tỉnh.

2. Sở Thông tin và Truyền thông thành lập đoàn kiểm tra tiến hành kiểm tra đột xuất các cơ quan, đơn vị, tổ chức, doanh nghiệp, cá nhân có dấu hiệu vi phạm an toàn, an ninh thông tin.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 21. Khen thưởng và xử lý vi phạm

1. Hàng năm, Sở Thông tin và Truyền thông dựa trên kết quả của công tác kiểm tra, điều tra, báo cáo của các tổ chức, cá nhân để đề xuất Ủy ban nhân dân tỉnh xem xét khen thưởng theo quy định; phê bình đối với những tổ chức, cá nhân vi phạm hoặc không thực hiện.

2. Các tổ chức, cá nhân vi phạm hoặc không thực hiện Quy chế này tùy theo tính chất, mức độ vi phạm sẽ bị xử lý theo quy định.

Điều 22. Tổ chức thực hiện

1. Sở Thông tin và Truyền thông chủ trì, phối hợp với các cơ quan, đơn vị có liên quan triển khai thực hiện tốt Quy chế này.

2. Thủ trưởng các cơ quan, đơn vị, tổ chức, doanh nghiệp liên quan trên địa bàn tỉnh tổ chức triển khai thực hiện nghiêm túc Quy chế này tại cơ quan, đơn vị và báo cáo định kỳ hàng năm cho Ủy ban nhân dân tỉnh *(thông qua sở Thông tin và Truyền thông)*. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, phát sinh cần sửa đổi, bổ sung, đề nghị các cơ quan, đơn vị kịp thời báo cáo về Sở Thông tin và Truyền thông để tổng hợp trình Ủy ban nhân dân tỉnh xem xét, quyết định./.

TM. UỶ BAN NHÂN DÂN
CHỦ TỊCH

Phạm Ngọc Nghị