ỦY BAN NHÂN DÂN TỈNH BẮC GIANG	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 176/2012/QĐ-UBND	*Bắc Giang, ngày 18 tháng 6 năm 2012*

QUYẾT ĐỊNH
Ban hành Quy định đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Bắc Giang

ỦY BAN NHÂN DÂN TỈNH BẮC GIANG

Căn cứ Luật Tổ chức HĐND và UBND ngày 26 tháng 11 năm 2003;

Căn cứ Luật Ban hành văn bản quy phạm pháp luật của HĐND, UBND ngày 14 tháng 12 năm 2004;

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

Căn cứ Pháp lệnh bảo vệ bí mật nhà nước ngày 28 tháng 12 năm 2000;

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 Sở Thông tin và Truyền thông tại Tờ trình số 07/TTr-STTTT, ngày 17 tháng 5 năm 2012,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy định đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Bắc Giang.

Điều 2. Quyết định này có hiệu lực sau 10 ngày, kể từ ngày ký.

Điều 3. Giám đốc Sở, Thủ trưởng các cơ quan, đơn vị thuộc Ủy ban nhân dân tỉnh; Chủ tịch Ủy ban nhân dân huyện, thành phố và các cơ quan, đơn vị, cá nhân liên quan căn cứ Quyết định thi hành./.

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

Bùi Văn Hạnh

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

QUY ĐỊNH
Đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Bắc Giang

(Ban hành kèm theo Quyết định số 176/2012/QĐ-UBND ngày 18/6/2012 của Ủy ban nhân dân tỉnh Bắc Giang)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh: Quy định này quy định về đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin (CNTT) của các cơ quan nhà nước tỉnh Bắc Giang.

2. Đối tượng áp dụng: Cơ quan quản lý nhà nước và đơn vị sự nghiệp (sau đây gọi chung là cơ quan nhà nước) trên địa bàn tỉnh Bắc Giang; cán bộ, công chức, viên chức và người lao động tham gia vào việc vận hành, khai thác và sử dụng hệ thống thông tin của các cơ quan nhà nước.

Điều 2. Giải thích từ ngữ

1. Môi trường mạng bao gồm: mạng nội bộ (LAN), mạng tin học diện rộng của Ủy ban nhân dân tỉnh (WAN), mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước, mạng riêng ảo (VPN), mạng Internet.

2. Các vùng trong hệ thống mạng bao gồm:

a) Vùng ngoài (Public Zone): là vùng Internet;

b) Vùng DMZ (DMZ - DeMilitarized Zone): là một vùng mạng trung lập giữa mạng nội bộ và mạng internet, chứa các thông tin cho phép người dùng từ internet truy xuất vào mạng nội bộ và chấp nhận các rủi ro tấn công từ internet. Các thiết bị tại vùng này bao gồm các thiết bị mạng phục vụ cho vùng và các máy chủ ứng dụng;

c) Vùng làm việc (Working Zone): là vùng mạng cục bộ của cơ quan và nơi bố trí các mạng nội bộ ảo trực thuộc mạng nội bộ của đơn vị. Các mạng nội bộ ảo này có thể kết nối với nhau thông qua lớp trung gian hoặc kết nối trực tiếp với nhau.

3. Những tài liệu thuộc bí mật nhà nước gồm:

a) Những thông tin tài liệu thuộc danh mục bí mật nhà nước đã được Thủ tướng Chính phủ, Bộ trưởng Bộ Công an quyết định có liên quan đến hoạt động của các cơ quan, tổ chức trên địa bàn tỉnh Bắc Giang;

b) Tài liệu mật do các cơ quan, tổ chức tỉnh xác lập, phát hành trên cơ sở danh mục bí mật nhà nước đã được duyệt;

c) Tài liệu mật do các cơ quan, tổ chức của Bộ, ngành Trung ương và địa phương khác chuyển đến cơ quan, tổ chức trong tỉnh.

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

5. Đảm bảo an toàn, an ninh thông tin: là việc bảo vệ thông tin số và hệ thống thông tin chống lại các nguy cơ tự nhiên hoặc do con người gây ra nhằm bảo đảm cho các hệ thống thông tin thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy. Nội dung đảm bảo an toàn, an ninh thông tin bao gồm bảo vệ an toàn mạng và hạ tầng thông tin, an toàn máy tính, dữ liệu và ứng dụng công nghệ thông tin.

Chương II
NỘI DUNG ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 3. Mạng nội bộ

1. Mô hình mạng

Hệ thống mạng nội bộ của các cơ quan phải được thiết kế thành một thể thống nhất, cùng kết hợp và hỗ trợ, tương tác hoạt động với nhau. Mô hình mạng tại các đơn vị phải được đảm bảo đầy đủ chia thành ba vùng gồm: vùng ngoài, vùng DMZ, vùng làm việc. Hệ thống mạng tại mỗi cơ quan phải được xây dựng theo mô hình miền (Domain) nhằm mục đích quản lý hệ thống chặt chẽ, an toàn và bảo mật.

2. Cấu hình mạng

Các thiết bị mạng, máy chủ, được đặt riêng biệt trong phòng máy chủ để đảm bảo tính an toàn, bảo mật và tập trung, tạo thuận lợi cho việc quản trị hệ thống. Máy chủ phải được đặt trong vùng DMZ của bức tường lửa. Thiết bị chuyển mạch lớp 3 (switch layer 3) đóng vai trò trung tâm kết nối của hệ thống mạng, thiết bị chuyển mạch lớp 3 được đặt tại phòng máy chủ kết nối các thiết bị chuyển mạch lớp 2 đặt tại mỗi tầng của đơn vị tạo thành hệ thống mạng nội bộ tổng thể.

3. Mạng không dây

Ngoài giải pháp mạng có dây, các cơ quan có thể xây dựng giải pháp mạng nội bộ kết hợp với mạng không dây. Hệ thống mạng không dây phải đáp ứng theo chuẩn N, với tốc độ 100Mb/giây (Mbps) và được bảo mật truy cập theo chuẩn bảo mật mạng không dây an toàn nhất hiện nay là WPA2. Khi thiết lập mạng không dây để kết nối với mạng cục bộ thông qua các điểm truy nhập (Access Point), cần thiết lập các tham số như: tên, SSID, mật khẩu, mã hóa dữ liệu và thông báo các thông tin liên quan đến Access Point để cơ quan sử dụng, định kỳ 3 tháng thay đổi mật khẩu nhằm tăng cường công tác bảo mật.

Điều 4. Trang thiết bị và hạ tầng công nghệ thông tin

1. Phòng máy chủ

Phòng máy chủ của các cơ quan phải độc lập, bộ phận chuyên trách hay cán bộ chuyên trách công nghệ thông tin trực tiếp quản lý, các cán bộ không có liên quan không được vào phòng máy chủ. Phòng máy chủ phải đảm bảo khô, thoáng, nguồn

điện cung cấp đảm bảo tính ổn định cao. Phòng máy chủ phải được trang bị máy lạnh và vận hành máy lạnh liên tục.

2. Máy chủ

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

3. Thiết bị chống sét

Các cơ quan phải lắp đặt thiết bị chống sét để bảo vệ hệ thống CNTT, phải xây dựng ít nhất 02 thiết bị chống sét: một cho một đường cung cấp điện và một đường của mạng nội bộ (LAN).

4. Thiết bị chuyển mạch (Switch)

Thiết bị chuyển mạch mạng tin học của các cơ quan phải đảm bảo 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 trên từng cổng, quy định địa chỉ IP cho từng cổng 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 có hỗ trợ định tuyến IP (IP Routing) cho mỗi mạng nội bộ, hỗ trợ chức năng điều khiển truy cập (Access Control List), hỗ trợ chức năng xác thực thiết bị và người sử dụng (User & Device Authentication) và chức năng bảo mật quản trị mạng (Network Administration Security).

5. Bức tường lửa (Firewall)

Các cơ quan phải xây dựng Firewall đảm bảo các yêu cầu gồm khả năng xử lý được số lượng kết nối đồng thời cao và chịu được thông lượng cao, hỗ trợ các công nghệ mạng riêng ảo thông dụng và có phần cứng mã hóa tích hợp để tăng tốc độ mã hóa dữ liệu, cung cấp đầy đủ các cơ chế bảo mật cơ bản như NAT, PAT, quản lý luồng dữ liệu ra, vào và có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ (DoS).

Điều 5. Quy định về đầu tư và quản trị phần mềm

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

1. Quản lý tài nguyên: Cán bộ quản trị mạng có trách nhiệm kiểm tra, giám sát chức năng chia sẻ thông tin (Network File and Folder Sharing); tổ chức cấp phát tài nguyên trên máy chủ theo danh mục thư mục cho từng phòng/ban; khuyến cáo người sử dụng 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 việc 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 khóa 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 pháp 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 thường xuyên mật khẩu.

3. Quản lý tài khoản: Các tài khoản và định danh người dùng trong 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 nhập hệ thống thông tin đối với cán bộ, nhân viên đã chuyển công tác hoặc chấm dứt hợp đồng lao động.

4. Quản lý Logfile: 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 (backup) các logfile theo từng tháng để lưu vết theo dõi, xác định những sự kiện đã xảy ra của hệ thống và hạn chế việc tràn logfile gây ảnh hưởng đến hoạt động của hệ thống.

5. Chống mã độc, virus: Trên các máy chủ, các thiết bị di động trong mạng và những hệ thống thông tin quan trọng như: cổng (trang) thông tin điện tử, thư điện tử, một cửa điện tử,... phải cài đặt các phần mềm chống virus, thư rác phù hợp để phát hiện, loại trừ những đoạn mã độc hại (virus, trojan, worms,...) và hỗ trợ người sử dụng cài đặt các phần mềm này trên máy trạm.

Cán bộ quản trị mạng phải thường xuyên cập nhật các phiên bản (version) mới, các bản vá lỗi của các phần mềm chống virus để bảo đảm chương trình quét virus của cơ quan trên các máy chủ, máy trạm luôn được cập nhật mới nhất, thực hiện chế độ quét thường xuyên ít nhất là hàng tuần.

Điều 6. Bảo vệ bí mật nhà nước trong ứng dụng công nghệ thông tin

1. Quy định về soạn thảo, in ấn, phát hành và sao chụp tài liệu mật

a) Không được sử dụng máy tính nối mạng Internet (hoặc máy tính để chế độ wifi) để soạn thảo văn bản, chuyển giao, lưu trữ thông tin có nội dung bí mật nhà nước; cung cấp tin, tài liệu và đưa thông tin bí mật nhà nước trên trang thông tin điện tử. Nghiêm cấm cài cắm các thiết bị lưu trữ tài liệu có nội dung bí mật nhà nước vào máy tính nối mạng Internet;

b) Không được in, sao chụp tài liệu, vật mang 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 để soạn thảo văn bản mật, các cơ quan phải chuyển cho Sở Thông tin và Truyền thông xử lý. Không được cho phép bất kỳ các công ty tư nhân hoặc người không có trách nhiệm trực tiếp sửa chữa, xử lý và khắc phục các sự cố của máy tính dùng để soạn thảo văn bản mật.

3. Trước khi thanh lý các máy tính trong các cơ quan nhà nước, cán bộ chuyên trách CNTT phải dùng các chương trình phần mềm xóa bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

Điều 7. Đảm bảo an toàn cho Cổng/trang thông tin điện tử (gọi tắt là web)

1. Xác định cấu trúc thiết kế web

Quản lý toàn bộ các phiên bản của mã nguồn, phối hợp với đơn vị thực hiện dịch vụ hosting tổ chức mô hình trang web hợp lý, tránh khả năng tấn công leo thang đặc quyền. Yêu cầu đơn vị cung cấp dịch vụ hosting phải cài đặt các hệ thống phòng vệ như tường lửa (firewall), thiết bị phát hiện/phòng chống xâm nhập (IDS/IPS) ở mức ứng dụng web (WAP- Web Application Firewall).

2. Vận hành ứng dụng web an toàn

Các trang web khi đưa vào sử dụng hoặc khi bổ sung thêm các chức năng, dịch vụ công mới cần đánh giá kiểm định nhằm tránh được các lỗi bảo mật thường xảy ra trên ứng dụng web như: SQL Injection, Cross-Site Scripting (xss), Broken Authentication and Session Management, Security Misconfiguration, Failure to Restrict URL Access, Insecure Cryptographic Storage, Insufficient Transport Layer Protection, Invalidated Redirects and Forwards,...

3. Phối hợp với các nhà cung cấp dịch vụ hosting xây dựng phương án phục hồi trang web, trong đó chú ý mỗi tháng thực hiện việc backup toàn bộ nội dung trang web một lần bao gồm mã nguồn, cơ sở dữ liệu, dữ liệu phi cấu trúc,... để bảo đảm khi có sự cố có thể khắc phục lại ngay trong vòng 24 giờ.

Điều 8. Cán bộ quản trị mạng

1. Yêu cầu về trình độ và phẩm chất

Cán bộ được giao quản lý, vận hành mạng phải được đào tạo chuyên môn, nắm vững kiến thức để quản trị mạng. Tối thiểu cán bộ quản trị mạng phải có trình độ cao đẳng CNTT trở lên, có chứng chỉ về an toàn, an ninh thông tin.

Đảm bảo an toàn, an ninh thông tin cho các hệ thống CNTT đòi hỏi các cơ quan tuyển dụng cán bộ quản trị mạng phải có phẩm chất đạo đức và phẩm chất chính trị.

2. Trách nhiệm quản trị

Cán bộ quản trị mạng là người chịu trách nhiệm về sự an toàn và an ninh thông tin trong cơ quan; chịu sự quản lý về chuyên môn nghiệp vụ của Sở Thông tin và Truyền thông; phải tham mưu xây dựng hệ thống và vận hành hệ thống CNTT của cơ quan tuân thủ các quy định về an toàn và an ninh thông tin.

Điều 9. Đảm bảo an toàn dữ liệu

1. Thiết lập và cấu hình cơ sở dữ liệu an toàn

a) Hệ quản trị cơ sở dữ liệu phải thường xuyên cập nhật bản vá lỗi mới nhất; sử dụng công cụ để đánh giá, tìm kiếm lỗ hổng trên máy chủ cơ sở dữ liệu;

b) Gỡ bỏ các cơ sở dữ liệu không sử dụng;

c) Thực hiện phân quyền và có quy định chặt chẽ với từng cá nhân truy cập đến cơ sở dữ liệu. Phải ghi nhật ký đối với các truy cập cơ sở dữ liệu, các thao tác đối với cấu hình cơ sở dữ liệu; Có các cơ chế sao lưu dữ liệu, tài liệu hóa quá trình thay đổi cấu trúc bằng cách xây dựng nhật ký cơ sở dữ liệu với các nội dung như: nội dung thay đổi, lý do thay đổi, thời gian, vị trí thay đổi,...

2. Thiết lập cơ chế sao lưu và phục hồi máy chủ, máy trạm

a) Đối với máy chủ: Cài đặt các dịch vụ Mirror, Raid, Clustering bảo đảm thiết lập cơ chế sao lưu và phục hồi hệ thống của máy chủ. Đối với các máy chủ cài đặt hệ điều hành Windows sử dụng chức năng System Restore để có thể dễ dàng khôi phục lại toàn bộ máy chủ hoặc các tập tin, thư mục được lựa chọn phục hồi;

b) Đối với máy trạm: Thực hiện việc sao lưu dữ liệu như hệ điều hành, các phần mềm ứng dụng văn phòng, phần mềm chuyên ngành,... bằng các phần mềm như Pqmagic, FinalData, Symantec Ghost,...

Điều 10. Giải quyết và khắc phục sự cố về an toàn, an ninh thông tin

1. Trách nhiệm của người sử dụng

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

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

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

a) Xử lý khẩn cấp: Khi phát hiện hệ thống bị tấn công, thông qua các dấu hiệu như luồng tin (traffic) tăng lên bất ngờ, nội dung trang chủ 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 logfile và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ;

Bước 3: Khôi phục hệ thống bằng cách chuyển dữ liệu backup mới nhất để hệ thống hoạt động.

b) Trong trường hợp sự cố xảy ra ngoài khả năng giải quyết của cơ quan phải báo cáo khẩn cấp bằng điện thoại cho Sở Thông tin và Truyền thông để được hỗ trợ, hướng dẫn và phối hợp khắc phục sự cố; đồng thời tham mưu văn bản báo cáo sự cố gửi Sở Thông tin và Truyền thông, Công an tỉnh.

3. Trách nhiệm của cơ quan chuyên trách CNTT

Sở Thông tin và Truyền thông là cơ quan chuyên trách CNTT của UBND tỉnh, có trách nhiệm đảm bảo an toàn, an ninh thông tin cho các hệ thống CNTT của các cơ quan nhà nước trong toàn tỉnh như sau:

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

b) Hỗ trợ, phối hợp và hướng dẫn các cơ quan 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 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 các nguyên nhân gây ra sự cố mất an toàn, an ninh thông tin khi có chỉ đạo của Ủy ban nhân dân tỉnh;

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

Chương III
TỔ CHỨC THỰC HIỆN

Điều 11. Trách nhiệm của Sở Thông tin và Truyền thông

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

2. Chủ trì, phối hợp với các cơ quan chức năng liên quan để thành lập đoàn kiểm tra định kỳ hàng năm hoặc đột xuất công tác đảm bảo an toàn, an ninh thông tin, triển khai kiểm tra và báo cáo Ủy ban nhân dân tỉnh kết quả kiểm tra.

3. Tiến hành xử phạt theo thẩm quyền đối với các hành vi vi phạm an toàn, an ninh thông tin gây thiệt hại cho hệ thống thông tin của các cơ quan nhà nước trên địa bàn tỉnh.

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

5. Tổng hợp báo cáo và thông báo về tình hình an toàn, an ninh thông tin định kỳ cho Ủy ban nhân dân tỉnh và các cơ quan có liên quan.

Điều 12. Trách nhiệm của Công an tỉnh

1. Chủ trì, phối hợp với Sở Thông tin và Truyền thông và các cơ quan có liên quan thực hiện quản lý, kiểm soát, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống thông tin xâm phạm đến an ninh chính trị, trật tự an toàn xã hội.

2. Thường xuyên thông báo cho các cơ quan về phương thức, thủ đoạn mới của các loại tội phạm xâm phạm an toàn, an ninh thông tin để có biện pháp phòng ngừa, ngăn chặn.

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

Điều 13. Trách nhiệm của các cơ quan nhà nước

1. Xây dựng quy chế nội bộ bảo đảm an toàn, an ninh thông tin

Các cơ quan phải ban hành quy chế nội bộ quy định rõ các vấn đề sau:

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

b) Quy định về cấp phát, thu hồi, cập nhật và quản lý các tài khoản truy cập vào hệ thống thông tin;

c) Quy định về an toàn, an ninh thông tin trên môi trường mạng trong nội bộ, cơ chế sao lưu dữ liệu, cơ chế thông tin, báo cáo và phối hợp khắc phục sự cố;

d) Quy định về quản trị hệ thống thông tin, quản lý và điều hành máy chủ, thiết bị mạng, thiết bị bảo vệ mạng một cách an toàn; quản lý phân quyền và trách nhiệm đối với từng cá nhân khi tham gia sử dụng hệ thống thông tin.

2. Đầu tư xây dựng và quản lý hệ thống CNTT

a) Các cơ quan trong đầu tư xây dựng hệ thống CNTT phải đáp ứng các yêu cầu bảo đảm an toàn, an ninh của hệ thống, nhằm giảm thiểu các nguy cơ gây ra sự cố, tạo điều kiện cho việc khắc phục và truy vết trong trường hợp có sự cố xảy ra;

b) Làm tốt công tác quản lý và vận hành hệ thống bảo vệ an toàn, an ninh thông tin; tiến hành kiểm tra đánh giá hoạt động của hệ thống bảo vệ an toàn, an ninh thông tin;

c) Định kỳ hàng năm (hoặc đột xuất khi xảy ra sự cố) tiến hành bảo trì và nâng cấp hệ thống bảo vệ an toàn, an ninh thông tin.

3. Phân công cán bộ có phẩm chất và năng lực chuyên môn quản trị mạng.

4. Tổ chức đào tạo tại cơ quan hoặc cử cán bộ tham gia các lớp đào tạo để trang bị các kiến thức về an toàn thông tin cơ bản cho cán bộ, công chức, viên chức trước khi cho phép truy nhập, vận hành, khai thác và sử dụng hệ thống thông tin.

5. Xác định và phân bổ kinh phí chi thường xuyên 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 spam, virus trên các máy trạm, máy chủ,...

6. Tạo điều kiện thuận lợi cho các cơ quan chức năng trong công tác kiểm tra về an toàn và an ninh thông tin; điều tra nguyên nhân gây ra sự cố; phân công cán bộ kỹ thuật tham gia khắc phục sự cố.

Điều 14. Điều khoản thi hành

1. Giao Sở Thông tin và Truyền thông chủ trì, phối hợp với các cơ quan liên quan đôn đốc, hướng dẫn triển khai thực hiện nghiêm túc Quy định này.

2. Các cơ quan và cán bộ công chức, viên chức và người lao động trong các cơ quan nhà nước trên địa bàn tỉnh vi phạm Quy định này tùy theo tính chất, mức độ vi phạm sẽ bị xử lý kỷ luật theo trách nhiệm, xử phạt hành chính, bồi thường thiệt hại hoặc bị truy cứu trách nhiệm hình sự theo các quy định hiện hành.

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

Bùi Văn Hạnh