UỶ BAN NHÂN DÂN **TỈNH VĨNH PHÚC**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 56 /2014/QĐ-UBND	*Vĩnh Yên, ngày 28 tháng 11 năm 2014*

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn thông tin, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước tỉnh Vĩnh Phúc

ỦY BAN NHÂN DÂN TỈNH

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

Căn cứ Luật Công nghệ thông tin số 67/2006/QH11 ngày 29/6/2006;

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 cơ quan nhà nước;

Căn cứ Nghị định số 72/2013/NĐ-CP ngày 15/7/2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng;

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 42/TTr-STTTT ngày 30/10/2014, văn bản thẩm định số 136/BC-STP ngày 28/10/2014 của Sở Tư pháp,

QUYẾT ĐỊNH:

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

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

Điều 3. Chánh Văn phòng UBND tỉnh; thủ trưởng các sở, ban, ngành; chủ tịch UBND huyện, thành phố, thị xã và các cá nhân, đơn vị liên quan có trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ Thông tin và Truyền thông;
- Cục KTVB - Bộ Tư pháp;
- TTTU, HĐND tỉnh, Đoàn ĐBQH tỉnh;
- Chủ tịch, các PCT; CPVP UBND tỉnh;
- UB MTTQ, các đoàn thể;
- Cổng thông tin điện tử Chính phủ;
- TT Công báo (để đăng);
- Báo Vĩnh Phúc, Đài PTTH tỉnh, Cổng TTĐT tỉnh;
- Lưu: VT, TH2.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Phạm Quang Hùng

UỶ BAN NHÂN DÂN **TỈNH VĨNH PHÚC**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**

QUY CHẾ

Bảo đảm an toàn thông tin, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước tỉnh Vĩnh Phúc

(Ban hành kèm theo Quyết định số 51/2014/QĐ-UBND ngày 28 tháng 11 năm 2014 của Ủy ban nhân dân tỉnh Vĩnh Phúc)

Chương I

QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về bảo đảm an toàn thông tin, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước tỉnh Vĩnh Phúc.

Điều 2. Đối tượng áp dụng

1. Quy chế này được áp dụng đối với các cơ quan nhà nước tỉnh Vĩnh Phúc và các tổ chức, cá nhân liên quan đến hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Vĩnh Phúc.

2. Khuyến khích các tổ chức, doanh nghiệp, cá nhân khác trên địa bàn tỉnh thực hiện Quy chế này.

Điều 3. Giải thích từ ngữ

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

1. *An toàn thông tin* là sự bảo vệ thông tin và các 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 việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

3. *Tường lửa* là tập hợp các thành phần hoặc một hệ thống các trang thiết bị, phần mềm được đặt giữa hai mạng, nhằm kiểm soát tất cả các kết nối từ bên trong ra bên ngoài mạng hoặc ngược lại.

4. *Hạ tầng kỹ thuật* là tập hợp thiết bị tính toán (máy chủ, máy trạm), thiết bị ngoại vi, thiết bị kết nối mạng, thiết bị phụ trợ, mạng nội bộ, mạng diện rộng.

5. *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.

6. *Mã độc* là một chương trình hoặc phần mềm được chèn một cách bí mật vào hệ thống với mục đích làm tổn hại đến tính bí mật, tính toàn vẹn hoặc tính sẵn sàng của hệ thống.

7. *Bản vá lỗ hổng bảo mật* của một phần mềm là công cụ được tạo ra để sửa một hoặc một số lỗi cụ thể đã hoặc có thể gây ra nguy cơ mất an toàn thông tin, an ninh thông tin khi sử dụng phần mềm.

Điều 4. Nguyên tắc bảo đảm an toàn thông tin

1. Việc bảo đảm an toàn thông tin, an ninh thông tin là yêu cầu bắt buộc trong quá trình thiết kế, xây dựng, vận hành, nâng cấp và hủy bỏ hạ tầng kỹ thuật, hệ thống thông tin của các cơ quan, đơn vị.

2. Các cơ quan chịu trách nhiệm bảo đảm an toàn thông tin, an ninh thông tin đối với thông tin và hệ thống thông tin thuộc thẩm quyền quản lý; chịu sự quản lý, thanh tra, kiểm tra và thực hiện các yêu cầu về bảo đảm an toàn thông tin, an ninh thông tin của cơ quan nhà nước có thẩm quyền.

3. Các cơ quan phải xây dựng quy định nội bộ về bảo đảm an toàn thông tin, an ninh thông tin; bố trí cán bộ chuyên trách, phụ trách quản lý an toàn thông tin, an ninh thông tin; quy định quyền hạn, trách nhiệm của thủ trưởng cơ quan, các bộ phận và cá nhân liên quan trong đơn vị đối với công tác bảo đảm an toàn thông tin, an ninh thông tin trong cơ quan.

Điều 5. Các hành vi bị cấm

1. Cản trở, ngăn chặn, can thiệp trái phép việc truyền tải thông tin, xóa, thay đổi, làm sai lệch thông tin trên mạng, ảnh hưởng tới sự hoạt động bình thường của hệ thống thông tin hoặc khả năng truy cập hợp pháp của người sử dụng tới hệ thống thông tin.

2. Sử dụng trái phép tài khoản, mật khẩu của tổ chức, cá nhân; thông tin riêng, thông tin cá nhân và tài nguyên Internet.

3. Khởi tạo, cài đặt, phát tán thư rác, tin nhắn rác, mã độc; thiết lập hệ thống thông tin lừa đảo, giả mạo.

4. Tấn công, chiếm quyền điều khiển, làm mất tác dụng của các biện pháp bảo vệ an toàn thông tin, an ninh thông tin; thu thập thông tin trái phép đối với hệ thống thông tin.

5. Lợi dụng mạng để truyền bá thông tin, quan điểm, tài liệu, hình ảnh, âm thanh hoặc dạng thông tin khác nhằm thực hiện các hành vi gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội.

6. Hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, cá nhân.

CHƯƠNG II
CÁC NỘI DUNG BẢO ĐẢM AN TOÀN THÔNG TIN, AN NINH THÔNG TIN VÀ PHƯƠNG THỨC THỰC HIỆN

Điều 6. Bảo đảm an toàn vật lý và môi trường

1. Các khu vực xử lý, lưu trữ thông tin, phương tiện xử lý thông tin, phương tiện bảo đảm an toàn thông tin phải được đặt ở vị trí an toàn, bảo vệ bằng tường bao và kiểm soát ra vào, bảo đảm chỉ có người có nhiệm vụ mới được vào và phải có nội quy riêng khi làm việc trong các khu vực này.

2. Các khu vực tại khoản 1, Điều này phải có biện pháp bảo vệ phòng chống cháy nổ, ngập lụt, động đất, tác động của môi trường và các thảm họa khác do thiên nhiên và con người gây ra.

3. Khu vực an toàn, bảo mật phải được kiểm soát và cách ly với khu vực sử dụng chung.

4. Bảo đảm thiết bị lưu trữ dữ liệu quan trọng, phần mềm bản quyền lưu trữ trên thiết bị phải được kiểm tra, xóa hoặc ghi đè không có khả năng khôi phục trước khi loại bỏ hoặc tái sử dụng cho mục đích khác.

Điều 7. Bảo đảm an toàn trong phát triển hệ thống thông tin, trao đổi thông tin trên môi trường mạng

1. Khi xây dựng mới hệ thống thông tin hoặc cải tiến hệ thống thông tin hiện tại, phải đưa ra các yêu cầu về an toàn, bảo mật cho hệ thống.

2. Khuyến khích áp dụng công nghệ mã hóa, chữ ký số khi chia sẻ, lưu trữ, trao đổi thông tin trên môi trường mạng.

3. Phân loại thông tin theo các tiêu chí về giá trị và tầm quan trọng, tần suất sử dụng, thời gian lưu trữ để áp dụng phương thức bảo vệ thích hợp.

4. Việc gửi thông tin trên mạng phải bảo đảm:

a) Không giả mạo nguồn gốc của thông tin;

b) Tuân thủ Quy chế này và quy định của pháp luật có liên quan.

5. Khi cần kết nối từ xa vào máy chủ để quản trị, phải sử dụng phương thức kết nối có mã hóa.

6. Sử dụng Mạng truyền số liệu chuyên dùng của tỉnh để truy cập, khai thác các hệ thống thông tin dùng chung của tỉnh.

7. Chỉ sử dụng thư điện tử công vụ và các công cụ trao đổi thông tin do các cơ quan Nhà nước hoặc tổ chức có thẩm quyền cung cấp để trao đổi thông tin, tài liệu trong hoạt động công vụ. Không sử dụng các phương tiện trao đổi thông tin công cộng trên Internet cho mục đích này.

Điều 8. Quản lý truy cập

1. Các hệ thống thông tin, mạng phải sử dụng tường lửa để ngăn chặn và phát hiện các xâm nhập trái phép vào hệ thống nội bộ.

2. Phải có quy định về quản lý truy cập vào hệ thống thông tin, mạng tại mỗi đơn vị.

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

4. Mỗi cán bộ, công chức, viên chức và người lao động chỉ được phép truy cập thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình.

5. Các hệ thống thông tin phải giới hạn số lần đăng nhập sai liên tiếp vào hệ thống. Thiết lập chế độ tự động khoá tạm thời tài khoản nếu liên tục đăng nhập sai vượt quá số lần quy định.

6. Hủy bỏ quyền truy cập vào hệ thống thông tin, thu hồi lại tất cả các tài sản liên quan tới hệ thống thông tin của cơ quan (khoá, thẻ nhận dạng, thư mục lưu trữ, thư điện tử công vụ, máy vi tính, tài khoản) khi cán bộ, công chức, viên chức và người lao động chuyển công tác, nghỉ hưu hoặc chấm dứt lao động hợp đồng.

7. Tất cả máy trạm, máy chủ phải được đặt mật khẩu truy cập và thiết lập chế độ tự động bảo vệ màn hình sau tối đa 10 phút không sử dụng.

8. Khi thiết lập mạng không dây trong nội bộ đơn vị, phải đặt mật khẩu truy cập vào mạng không dây và chỉ cho phép truy cập dịch vụ Internet.

9. Mật khẩu truy cập vào các hệ thống thông tin phải có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự-số và ký tự đặc biệt) và không quá 03 tháng phải đổi một lần.

10. Không đặt chế độ tự động lưu trữ mật khẩu trong các trình duyệt trong mọi trường hợp sử dụng.

Điều 9. Phòng chống mã độc

1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống mã độc. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin.

2. Thiết lập chế độ tự động cập nhật bản vá lỗ hổng bảo mật cho phần mềm hệ điều hành, các phần mềm ứng dụng và hệ quản trị cơ sở dữ liệu được cài đặt trên máy chủ.

3. Cán bộ, công chức, viên chức và người lao động không được tự ý gỡ bỏ các phần mềm phòng chống mã độc trên máy tính trạm khi chưa có sự đồng ý của người có thẩm quyền theo quy định của cơ quan.

4. Tất cả các máy tính của đơn vị phải được cấu hình vô hiệu hóa tính năng tự động thực thi (autoplay) các tập tin trên các thiết bị lưu trữ di động.

5. Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng.

6. Máy chủ chỉ được dùng để cài đặt các phần mềm, dịch vụ dùng chung của cơ quan, đơn vị; không cài đặt phần mềm không rõ nguồn gốc, phần mềm không có nhu cầu sử dụng trên máy chủ.

7. Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm mã độc trên máy trạm người sử dụng phải báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý.

Điều 10. Sao lưu dữ liệu dự phòng

1. Ban hành và thực hiện quy trình sao lưu dữ liệu dự phòng và phục hồi cho các hệ thống thông tin và dữ liệu cần thiết.

2. Dữ liệu quan trọng của cơ quan phải được sao lưu, bao gồm: thông tin cấu hình và tập tin nhật ký của của các thiết bị mạng, bảo mật, hệ điều hành; phần mềm ứng dụng, cơ sở dữ liệu. Thời gian sao lưu được thực hiện hằng ngày.

3. Ngoài các quy định tại khoản 2 Điều này, các cơ quan phải lập danh sách dữ liệu cần sao lưu, phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra khả năng phục hồi hệ thống từ dữ liệu sao lưu.

4. Dữ liệu sao lưu phải được lưu trữ an toàn và được kiểm tra thường xuyên bảo đảm khả năng sẵn sàng cho việc sử dụng khi cần. Kiểm tra khả năng phục hồi hệ thống từ dữ liệu sao lưu tối thiểu 3 tháng một lần.

Điều 11. Quản lý nhật ký trong quá trình vận hành hệ thống thông tin

1. Các cơ quan phải thực hiện việc ghi nhật ký (log) trên các thiết bị mạng, bảo mật, máy chủ, phần mềm ứng dụng, hệ điều hành, cơ sở dữ liệu. Bảo đảm các sự kiện xảy ra đều được ghi nhận và lưu giữ. Thời gian ghi nhật ký tối thiểu 30 ngày.

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

3. Các công việc tối thiểu cần phải được ghi nhật ký gồm: quá trình truy cập hệ thống; tạo, cập nhật hoặc xóa dữ liệu; các hành vi xem, thiết lập cấu hình hệ thống; việc thiết lập các kết nối bất thường vào và ra hệ thống; thay đổi quyền truy cập hệ thống.

4. Thường xuyên theo dõi nhật ký của hệ thống và các sự kiện khác có liên quan để đánh giá, báo cáo mức độ nghiêm trọng của các rủi ro có thể xảy ra.

Điều 12. 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;

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;

c) Cao: sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và có ảnh hưởng đến hoạt động của cơ quan;

d) Khẩn cấp: sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của cơ quan.

2. Khi có sự cố hoặc nguy cơ mất an toàn thông tin, lãnh đơn vị phải chỉ đạo kịp thời để khắc phục và hạn chế thiệt hại, báo cáo nhanh và sau đó báo cáo bằng văn bản cho cơ quan cấp trên trực tiếp quản lý và Sở Thông tin và Truyền thông.

3. Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của đơn vị, lãnh đạo đơn vị phải chỉ đạo sao chép các tập tin nhật ký, tạm dừng hoạt động của hệ thống đồng thời báo cáo khẩn cấp cho cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ.

4. Quá trình xử lý sự cố phải được ghi chép và lưu trữ tại đơn vị; bảo toàn bằng chứng, chứng cứ phục vụ cho việc kiểm tra, xử lý, khắc phục và phòng ngừa sự cố. Trong trường hợp sự cố có liên quan đến các vi phạm pháp luật, đơn vị có trách nhiệm thu thập và cung cấp chứng cứ cho cơ quan có thẩm quyền đúng theo quy định của pháp luật

Điều 13. Quy định sử dụng các hệ thống thông tin dùng chung của tỉnh

1. Các hệ thống thông tin dùng chung của tỉnh được cài đặt tại Trung tâm Hạ tầng thông tin gồm:

a) Hệ thống Cổng Thông tin - Giao tiếp điện tử của tỉnh; các cổng thông tin điện tử thành phần của các cơ quan, đơn vị; các dịch vụ công trực tuyến;

b) Hệ thống phần mềm quản lý văn bản và điều hành;

c) Hệ thống thư điện tử công vụ của tỉnh;

d) Hệ thống một cửa điện tử;

e) Hệ thống người dùng tập trung toàn tỉnh;

f) Hệ thống phân giải tên miền nội bộ của tỉnh (Hệ thống DNS);

g) Các hệ thống thông tin khác có chức năng liên thông, tích hợp, luân chuyển dữ liệu giữa các cơ quan nhà nước của tỉnh.

2. Nghiêm cấm tiết lộ tài khoản truy cập, đấu nối, truy cập trái phép vào các hệ thống thông tin dùng chung của tỉnh;

3. Tài khoản truy cập các hệ thống thông tin dùng chung của tỉnh phải đổi mật khẩu mặc định ngay sau khi được Sở Thông tin và Truyền thông cấp. Mật khẩu phải được thay đổi định kỳ hàng tháng và được đặt theo quy định tại khoản 9, Điều 8 Quy chế này.

Điều 14. Bảo vệ bí mật Nhà nước trong trong hoạt động ứng dụng công nghệ thông tin

1. Không được sử dụng máy tính nối mạng để soạn thảo văn bản, chuyển giao, lưu trữ thông tin có nội dung thuộc bí mật nhà nước; cung cấp tin, tài liệu và thông tin bí mật nhà nước trên mạng.

2. Không được in, sao chụp tài liệu bí mật nhà nước trên các thiết bị kết nối mạng.

3. Khi sửa chữa, khắc phục sự cố của máy tính dùng soạn thảo văn bản mật, các cơ quan phải báo cáo và có sự giám sát, quản lý chặt chẽ của cơ quan có thẩm quyền.

4. Có biện pháp quản lý chặt chẽ trong việc sử dụng và thanh lý tài sản, các trang thiết bị công nghệ thông tin lưu trữ các thông tin thuộc danh mục bí mật Nhà nước. Tuân thủ các quy định khác có liên quan của về công tác bảo vệ bí mật nhà nước.

Chương III

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

Điều 15. Trách nhiệm của cán bộ, công chức, viên chức và người lao động

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

a) Chấp hành các quy định, quy trình nội bộ, Quy chế này và các quy định khác của pháp luật về an toàn thông tin, an ninh thông tin. Chịu trách nhiệm bảo đảm an toàn thông tin, an ninh thông tin trong phạm vi trách nhiệm và quyền hạn được giao;

b) Cán bộ, công chức, viên chức và người lao động phải có trách nhiệm tự quản lý, bảo quản, bảo đảm an toàn cho các thiết bị mà mình được giao sử dụng;

c) Khi phát hiện sự cố mất an toàn thông tin, an ninh thông tin phải thông báo ngay với cấp trên và cán bộ chuyên trách, phụ trách công nghệ thông tin để kịp thời ngăn chặn, xử lý;

d) Tham gia đầy đủ các chương trình đào tạo, tập huấn về an toàn thông tin, an ninh thông tin do Ủy ban nhân dân tỉnh chỉ đạo.

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

Ngoài các quy định tại khoản 1 Điều này, cán bộ chuyên trách, phụ trách công nghệ thông tin có trách nhiệm:

a) Tham mưu lãnh đạo cơ quan ban hành các quy định, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin, an ninh thông tin;

b) Trực tiếp thiết lập các biện pháp kỹ thuật bảo đảm an toàn cho hạ tầng kỹ thuật, hệ thống thông tin trong cơ quan, đơn vị mình; hướng dẫn cán bộ, công chức, viên chức và người lao động trong cơ quan, đơn vị tuân thủ các biện pháp bảo đảm an toàn thông tin, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin;

c) Thực hiện việc giám sát, đánh giá, báo cáo thủ trưởng cơ quan các sự cố mất an toàn thông tin và mức độ nghiêm trọng của các sự cố đó;

d) Phối hợp với cá nhân, đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn thông tin, an ninh thông tin.

Điều 16. Trách nhiệm của các cơ quan

1. Thủ trưởng cơ quan, đơn vị có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong công tác bảo đảm an toàn thông tin, an ninh thông tin của đơn vị mình.

2. Phân công bộ phận hoặc cán bộ chuyên trách bảo đảm an toàn thông tin, an ninh thông tin của đơn vị; tạo điều kiện để các cán bộ phụ trách an toàn thông tin, an ninh thông tin được học tập, nâng cao trình độ về an toàn thông tin, an ninh thông tin; thường xuyên tổ chức quán triệt các quy định về an toàn thông tin, an ninh thông tin trong cơ quan; xác định các yêu cầu, trách nhiệm đảm bảo an toàn thông tin, an ninh thông tin đối với các vị trí cần tuyển dụng hoặc phân công; quy định trách nhiệm đảm bảo an toàn thông tin, an ninh thông tin trong các Quyết định tuyển dụng hoặc Hợp đồng lao động.

3. Ban hành quy định, quy trình nội bộ về bảo đảm an toàn thông tin, an ninh thông tin phù hợp với Quy chế này và các quy định của pháp luật.

4. Áp dụng mọi biện pháp để khắc phục và hạn chế thiệt hại do sự cố xảy ra, báo cáo sự cố cho cơ quan cấp trên trực tiếp quản lý và Sở Thông tin và Truyền thông theo quy định tại Điều 12 Quy chế này.

5. Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố an toàn thông tin, an ninh thông tin kịp thời, nhanh chóng và đạt hiệu quả.

6. Phối hợp chặt chẽ với Công an tỉnh, Sở Thông tin và Truyền thông và các đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin, an ninh thông tin.

7. Định kỳ hằng quý, lập báo cáo về tình hình an toàn thông tin, an ninh thông tin và gửi về Sở Thông tin và Truyền thông.

Điều 17. Trách nhiệm của Sở Thông tin và Truyền thông

1. Tham mưu UBND tỉnh về công tác bảo đảm an toàn thông tin, an ninh thông tin trên địa bàn tỉnh và chịu trách nhiệm trước UBND tỉnh trong việc bảo đảm an toàn thông tin, an ninh thông tin cho các hệ thống thông tin của tỉnh.

2. Hàng năm xây dựng kế hoạch, tổng hợp nhu cầu của các cơ quan, đơn vị để triển khai công tác an toàn thông tin, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước trên địa bàn tỉnh theo quy định.

3. Chủ trì, phối hợp với các cơ quan liên quan thành lập đoàn thanh, kiểm tra định kỳ hoặc đột xuất; kịp thời phát hiện và xử lý theo thẩm quyền đối với các hành vi vi phạm an toàn thông tin, an ninh thông tin trên địa bàn tỉnh.

4. Xây dựng và triển khai các chương trình đào tạo, hội nghị tuyên truyền về an toàn thông tin, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh.

5. Chỉ đạo các đơn vị chức năng hướng dẫn về nghiệp vụ quản lý vận hành, kỹ thuật bảo đảm an toàn thông tin, an ninh thông tin; hỗ trợ giải quyết sự cố khi có yêu cầu.

6. Hướng dẫn, giám sát các cơ quan, đơn vị trên địa bàn tỉnh xây dựng quy chế nội bộ và thực hiện việc bảo đảm an toàn thông tin, an ninh cho hệ thống thông tin theo quy định của Nhà nước.

7. Tổng hợp và báo cáo về tình hình an toàn thông tin, an ninh thông tin theo định kỳ cho Bộ Thông tin và Truyền thông, Ủy ban nhân dân tỉnh và các cơ quan, đơn vị có liên quan.

Điều 18. 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 xây dựng kế hoạch, kiểm soát, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống thông tin gây hại đến an toàn thông tin, an ninh thông tin trong cơ quan nhà nước.

2. Phối hợp với Sở Thông tin và Truyền thông trong công tác thanh tra, kiểm tra về an toàn thông tin, an ninh thông tin.

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

Điều 19. Trách nhiệm của Trung tâm Hạ tầng thông tin

1. Bảo đảm an toàn thông tin, an ninh thông tin cho hạ tầng kỹ thuật công nghệ thông tin, các hệ thống thông tin dùng chung của tỉnh; tài nguyên Internet của tỉnh; Mạng truyền số liệu chuyên dùng của tỉnh.

2. Thường xuyên rà soát, kiểm tra, đánh giá định kỳ hàng năm, hàng quý hạ tầng kỹ thuật công nghệ thông tin, hệ thống thông tin dùng chung của tỉnh.

3. Thường xuyên cập nhật các nguy cơ gây mất an toàn thông tin, an ninh thông tin và thông báo cho các cơ quan, đơn vị biết để có biện pháp phòng ngừa, ngăn chặn, xử lý kịp thời.

4. Là đầu mối để tiếp nhận, phối hợp, hỗ trợ các cơ quan, đơn vị giải quyết các sự cố mất an toàn thông tin, an ninh thông tin.

Chương IV

TỔ CHỨC THỰC HIỆN

Điều 20. Hình thức xử lý vi phạm

Các hành vi vi phạm Quy chế này, tùy theo mức độ vi phạm sẽ bị xử lý theo quy định của pháp luật.

Điều 21. Thủ trưởng Sở, Ban, Ngành, Chủ tịch UBND các huyện, thành phố, thị xã tổ chức triển khai Quy chế tại cơ quan, đơn vị, địa phương mình..

Điều 22. Sở Tài Chính, Sở Kế hoạch và Đầu tư đề xuất với UBND tỉnh bố trí kinh phí để thực hiện các nhiệm vụ bảo đảm an toàn thông tin, an ninh thông tin của tỉnh. Kịp thời bổ sung kinh phí ngoài dự toán theo kế hoạch khi phát sinh sự cố khẩn cấp, bảo đảm hệ thống nhanh chóng được khắc phục.

Điều 23. Trong quá trình thực hiện, nếu có những vấn đề cần sửa đổi, bổ sung, đề nghị các đơn vị gửi về Sở Thông tin và Truyền thông để tổng hợp, báo cáo UBND tỉnh xem xét, quyết định./.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Phùng Quang Hùng