ỦY BAN NHÂN DÂN TỈNH LAI CHÂU	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 04 /2016/QĐ-UBND	*Lai Châu, ngày 28 tháng 3 năm 2016*

QUYẾT ĐỊNH

Ban hành Quy định đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Lai Châu

ỦY BAN NHÂN DÂN TỈNH LAI CHÂU

Căn cứ Luật Tổ chức Chính quyền địa phương ngày 19/6/2015;

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

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

Căn cứ Luật Giao dịch điện tử ngày 29/11/2005;

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

Căn cứ Luật An toàn thông tin mạng ngày 19/11/2015;

Căn cứ Pháp lệnh bảo vệ bí mật Nhà nước ngày 28/12/2000;

Căn cứ Nghị định số 33/2002/NĐ-CP ngày 28/03/2002 của Chính phủ quy định chi tiết thi hành Pháp lệnh bảo vệ bí mật nhà nước;

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;

Xét đề nghị của Sở Thông tin và Truyền thông tại Tờ trình số 211/TTr-STTTT ngày 16/3/2016,

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 trên địa bàn tỉnh Lai Châu.

Điều 2. Giao Sở Thông tin và Truyền thông giúp UBND tỉnh đôn đốc các sở, ban, ngành, đoàn thể tỉnh, UBND các huyện, thành phố và các đơn vị có liên quan tổ chức, triển khai thực hiện Quyết định này.

Điều 3. Quyết định này có hiệu lực sau 10 ngày kể từ ngày ký. Chánh Văn phòng UBND tỉnh; Thủ trưởng các sở, ban, ngành, đoàn thể tỉnh; Chủ tịch UBND các huyện, thành phố và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Văn phòng Chính phủ;
- Bộ Thông tin và Truyền thông;
- Cục Kiểm tra VBQPPL-Bộ Tư pháp;
- TT.Tỉnh ủy, HĐND tỉnh;
- Đoàn ĐBQH tỉnh;
- Sở Tư pháp;
- Báo Lai Châu;
- Đài PT-TH tỉnh;
- Công báo tỉnh;
- Cổng Thông tin điện tử tỉnh;
- Lưu: VT, VX.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Đỗ Ngọc An

ỦY BAN NHÂN DÂN
TỈNH LAI CHÂU

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 trên địa bàn tỉnh Lai Châu

(Ban hành kèm theo Quyết định số: 04 /2016/QĐ-UBND ngày 28 /3/2016 của UBND tỉnh Lai Châu)

Chương I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy định này quy định về công tác đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin (CNTT) trên địa bàn tỉnh Lai Châu, bao gồm: Công tác quản lý đảm bảo an toàn, an ninh thông tin mạng, việc áp dụng các biện pháp quản lý kỹ thuật, quản lý vận hành đảm bảo an toàn, an ninh thông tin đối với các hệ thống thông tin.

Điều 2. Đối tượng áp dụng

1. Quy định này áp dụng đối với các sở, ban, ngành, đoàn thể tỉnh; Ủy ban nhân dân (UBND) các huyện, thành phố; các tổ chức chính trị, tổ chức chính trị - xã hội, tổ chức chính trị - xã hội - nghề nghiệp trên địa bàn tỉnh Lai Châu *(sau đây gọi tắt là các cơ quan, đơn vị)*.

2. Các cán bộ, công chức, viên chức *(sau đây gọi tắt là CBCCVC)*, người lao động trong cơ quan, đơn vị nêu tại Khoản 1 Điều này và các tổ chức, cá nhân có liên quan áp dụng quy định này trong việc vận hành, khai thác và sử dụng hệ thống thông tin tại các cơ quan, đơn vị.

3. Các tổ chức, doanh nghiệp cung cấp dịch vụ hạ tầng mạng, Internet, CNTT.

Điều 3. Giải thích từ ngữ

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

1. An toàn thông tin: 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. Việc bảo vệ thông tin, tài sản và con người trong hệ thống thông tin nhằm bảo đảm cho các hệ thống thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy. An toàn thông tin bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng.

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. Hệ thống thông tin: Là tập hợp các thiết bị viễn thông, CNTT, bao gồm phần cứng, phần mềm, và cơ sở dữ liệu phục vụ cho hoạt động lưu trữ, xử lý, truyền đưa, chia sẻ, trao đổi, cung cấp và sử dụng thông tin.

4. Thông tin số: Thông tin số là thông tin được tạo lập bằng phương pháp dùng tín hiệu số.

5. Mạng: Là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính.

6. 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.

7. 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.

8. Vi rút máy tính: Là chương trình máy tính có khả năng lây lan, gây ra hoạt động không bình thường cho thiết bị số hoặc sao chép, sửa đổi, xóa bỏ thông tin lưu trữ trong thiết bị số.

9. Phần mềm độc hại: Là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

10. Phòng máy chủ: Là nơi đặt tập trung các thiết bị CNTT dùng chung, như: máy chủ (Server), các thiết bị mạng, an toàn mạng,... của một cơ quan, đơn vị.

11. Máy trạm: Là máy tính cá nhân khi được kết nối với hệ thống mạng nội bộ của cơ quan, đơn vị.

12. 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 gây ra nguy cơ mất an toàn, an ninh thông tin khi sử dụng phần mềm.

13. Bản ghi nhật ký hệ thống (Logfile): Là một tập tin được tạo ra trên mỗi thiết bị của hệ thống thông tin như tường lửa, máy chủ ứng dụng,... có chứa tất cả thông tin về các hoạt động xảy ra trên thiết bị đó. Bản ghi nhật ký hệ thống dùng để phân tích những sự kiện đã xảy ra, nguồn gốc và các kết quả để có các biện pháp xử lý thích hợp.

14. Phần mềm: Là chương trình máy tính được mô tả bằng hệ thống ký hiệu, mã hoặc ngôn ngữ để điều khiển thiết bị số thực hiện chức năng nhất định.

15. Phần cứng: Là sản phẩm thiết bị số hoàn chỉnh; cụm linh kiện; linh kiện; bộ phận của thiết bị số, cụm linh kiện, linh kiện.

16. 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.

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

1. Các cơ quan, đơn vị phải phổ biến những kiến thức cơ bản về an toàn, an ninh thông tin cho CBCCVC và người lao động trước khi tham gia sử dụng hệ thống thông tin.

2. Việc bảo đảm an toàn, 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 cơ quan, đơn vị.

3. Hạ tầng kỹ thuật, hệ thống thông tin phải được định kỳ kiểm tra, đánh giá hoặc kiểm định về mặt an toàn, an ninh thông tin phù hợp các tiêu chuẩn, quy chuẩn kỹ thuật quy định.

4. Thông tin số thuộc quy định danh mục bí mật nhà nước của các cơ quan, đơn vị phải được phân loại, lưu trữ, bảo vệ trên cơ sở quy định của pháp luật về bảo vệ bí mật nhà nước.

5. Cơ quan, đơn vị phải ban hành quy định nội bộ về đảm bảo an toàn, an ninh thông tin; bố trí cán bộ chuyên trách, phụ trách quản lý an toàn, an ninh thông tin; quy định rõ quyền hạn, trách nhiệm của thủ trưởng đơn vị, các cấp, các bộ phận và từng cá nhân trong đơn vị đối với công tác đảm bảo an toàn, an ninh thông tin trong cơ quan, đơn vị.

Điều 5. Các hành vi bị nghiêm cấm

1. Ngăn chặn, cản trở trái phép việc truy cập, truyền tải thông tin trên mạng, can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật.

2. Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới khả năng truy nhập hệ thống thông tin của người sử dụng.

3. Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của các biện pháp bảo vệ an toàn, an ninh thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin, thu thập thông tin trái pháp luật.

4. Tạo, cài đặt, phát tán thư rác, tin nhắn rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.

5. Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân.

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

Điều 6. Đảm bảo an toàn mạng và hạ tầng kỹ thuật

1. Phòng máy chủ:

a) Các cơ quan, đơn vị phải bố trí phòng máy chủ độc lập, phân công bộ phận chuyên trách hoặc cán bộ phụ trách CNTT trực tiếp quản lý. Quá trình vào, ra phòng máy chủ phải được ghi nhận vào nhật ký quản lý phòng máy chủ;

b) Phòng máy chủ phải đảm bảo các điều kiện cho những thiết bị đặt trong đó hoạt động ổn định, các điều kiện tối thiểu gồm: được bố trí ở khu vực có điều kiện an ninh, tốt; khô ráo, có điều hòa không khí; nguồn cung cấp điện ổn định và có dự phòng; có bình chữa cháy hoặc hệ thống tự động cảnh báo, chữa cháy khẩn cấp; phòng, chống sét;

c) Trường hợp đặc biệt không bố trí được phòng máy chủ độc lập, có thể ghép chung với các bộ phận khác nhưng phải bố trí, lắp đặt hệ thống máy chủ và thiết bị mạng dùng chung trong tủ mạng (Rack) và đảm bảo các điều kiện cho các thiết bị này hoạt động theo quy định tại Điểm b Khoản 1 Điều này.

2. Thiết lập các cơ chế bảo vệ mạng nội bộ:

a) Khi có kết nối mạng nội bộ với mạng ngoài (như: internet, mạng cơ quan khác) cần sử dụng hệ thống phòng thủ, bảo vệ mạng nội bộ (như: thiết bị tường lửa chuyên dụng, phần mềm tường lửa);

b) Hệ thống mạng không dây (Wifi) phải được thiết lập mật khẩu truy cập đủ mạnh và phân lớp mạng riêng cho các máy tính truy cập mạng không dây, định kỳ thay đổi mật khẩu, chậm nhất ba tháng phải đổi một lần;

c) Tổ chức mô hình mạng nội bộ theo hướng sử dụng máy chủ để quản lý các máy trạm trong mạng, hạn chế sử dụng mô hình mạng không có máy chủ quản lý các máy trạm. Các cơ quan, đơn vị khi có nhu cầu kết nối mạng LAN của các đơn vị, bộ phận trực thuộc ở xa, không nằm trong cùng một khu vực cần sử dụng đường truyền riêng để tăng cường bảo mật dữ liệu trao đổi trên mạng;

d) Xây dựng và áp dụng các biện pháp bảo vệ, giám sát, ghi nhật ký hoạt động và quản lý hạ tầng kỹ thuật, hệ thống thông tin nhằm phòng ngừa, ngăn chặn và phát hiện sớm các truy cập trái phép;

đ) Thiết lập, cấu hình đầy đủ các tính năng của thiết bị an toàn mạng. Thường xuyên kiểm tra nhằm kịp thời phát hiện những dấu hiệu bất thường gây mất an toàn cho hệ thống mạng nội bộ của cơ quan, đơn vị;

e) Kiểm soát chặt chẽ việc cài đặt các phần mềm lên các máy chủ và máy trạm, đảm bảo tuân thủ quy định quản lý an toàn, an ninh thông tin của cơ quan, đơn vị và các quy định khác có liên quan;

g) Theo dõi thường xuyên tình trạng lây nhiễm và thực hiện loại bỏ phần mềm độc hại khỏi hệ thống thông tin.

3. An toàn cho máy chủ:

a) Thiết lập chế độ tự động cập nhật bản vá lỗ hổng bảo mật cho phần mềm hệ điều hành và các phần mềm ứng dụng được cài đặt trên máy chủ; đóng tất cả các cổng (Port) dịch vụ khi không sử dụng; thiết lập chính sách ghi lưu tập trong quá trình hoạt động (Log file) của mỗi máy chủ theo định kỳ từ 3 tháng trở lên;

b) Khi cần kết nối từ xa, nhất là từ Internet vào máy chủ để quản trị, phải sử dụng phương thức kết nối có mã hóa (ví dụ: SSH, VPN,...);

c) Các máy chủ chỉ dùng để cài đặt các phần mềm, dịch vụ dùng chung của cơ quan, đơn vị; không cài đặt các phần mềm không rõ nguồn gốc, phần

mềm không có nhu cầu sử dụng. Không sử dụng máy chủ để duyệt web đọc báo, xem tin tức, chơi điện tử,...;

d) Cài đặt phần mềm phòng, chống virus, mã độc cho tất cả các máy chủ, đồng thời đảm bảo các phần mềm phòng, chống virus, mã độc này luôn được cập nhật khả năng nhận dạng virus, mã độc mới từ nhà sản xuất.

4. An toàn khi sử dụng các thiết bị lưu trữ ngoài:

a) Việc sử dụng các thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB phải quét virus trước khi đọc hoặc sao chép dữ liệu;

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

Điều 7. An toàn dữ liệu, cơ sở dữ liệu

1. Các hệ thống phần mềm, cơ sở dữ liệu phải có cơ chế sao lưu dữ liệu dự phòng, dữ liệu được lưu trữ tại nơi an toàn, đồng thời phải thường xuyên kiểm tra để đảm bảo sẵn sàng phục hồi khi có sự cố xảy ra.

2. Sử dụng mật mã để bảo đảm an toàn và bảo mật dữ liệu trong lưu trữ và giao dịch theo quy định của Nhà nước về mật mã.

3. Quản lý chặt chẽ việc di chuyển các trang thiết bị CNTT lưu trữ dữ liệu, nhất là các thông tin thuộc danh mục bí mật Nhà nước.

4. Quản lý và phân quyền truy cập phần mềm và cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ của người sử dụng.

5. Phần mềm hệ quản trị cơ sở dữ liệu phải được thiết lập cơ chế tự động và thường xuyên cập nhật bản vá lỗ hổng bảo mật từ nhà sản xuất.

Điều 8. Đảm bảo an toàn trong hoạt động trao đổi thông tin trên mạng

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

a) Không giả mạo nguồn gốc của thông tin;

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

2. Phân loại tài sản thông tin theo các tiêu chí về giá trị, độ nhạy cảm và tầm quan trọng, tần suất sử dụng, thời gian lưu trữ.

3. Thực hiện các biện pháp quản lý phù hợp với từng loại tài sản thông tin đã phân loại

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

Điều 9. Bảo vệ bí mật Nhà nước trong công tác ứng dụng CNTT

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 đưa 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 các 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 trạng thiết bị CNTT lưu trữ các thông tin thuộc danh mục bí mật Nhà nước. Tuân thủ Pháp lệnh bảo vệ bí mật Nhà nước và các quy định khác có liên quan của Nhà nước về công tác bảo vệ bí mật nhà nước.

Điều 10. 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 người chuyên trách, phụ trách về 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 của đơn vị.

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

2. Đối với người chuyên trách, phụ trách về công nghệ thông tin:

a) Thông tin, báo cáo lãnh đạo cơ quan, đơn vị.

b) 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 (log file) 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.

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); đồng thời báo cáo sự cố và kết quả khắc phục sự cố cho Thủ trưởng cơ quan, đơn vị.

c) 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 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 và các đơn vị có liên quan.

Chương III

TRÁCH NHIỆM ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 11. Trách nhiệm của các cơ quan, đơn vị

1. Thủ trưởng các cơ quan, đơn vị chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong công tác đảm bảo an toàn, an ninh thông tin đối với toàn bộ hệ thống thông tin của đơn vị mình.

2. Thực hiện và chỉ đạo CBCCVC và người lao động thuộc thẩm quyền quản lý thực hiện nghiêm túc Quy định này.

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

4. Quan tâm đầu tư các thiết bị phần cứng, phần mềm liên quan đến công tác đảm bảo an toàn, an ninh thông tin.

5. Hủy bỏ quyền truy nhập vào hệ thống thông tin, thu hồi lại các tài liệu, hồ sơ, thông tin liên quan tới tài khoản của CBCCVC chuyển công tác, nghỉ hưu hoặc chấm dứt hợp đồng.

6. 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 bằng văn bản cho cơ quan có liên quan.

7. Phối hợp chặt chẽ với cơ quan Công an trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động vi phạm an toàn, an ninh thông tin.

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

Điều 12. Người chuyên trách, phụ trách công nghệ thông tin tại các cơ quan đơn vị

1. Được đào tạo, bồi dưỡng, học tập, nghiên cứu, tiếp thu 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 đảm bảo an toàn, an ninh thông tin mạng trong toàn hệ thống; triển khai 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 đảm bảo tính sẵn sàng, tin cậy và toàn vẹn.

7. Thường xuyên thực hiện phân tích, đánh giá và 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 và xây dựng phương án hạn chế, khắc phục các rủi ro và nguy cơ có thể xảy ra.

Điều 13. Đối với cán bộ, công chức, viên chức tại các cơ quan, đơn vị

a) Thường xuyên cập nhật chính sách, thủ tục an toàn thông tin của đơn vị và thực hiện hướng dẫn về an toàn, an ninh thông tin của cán bộ phụ trách;

b) Hạn chế việc sử dụng chức năng chia sẻ tài nguyên, nếu sử dụng chức năng này cần bật thuộc tính bảo mật bằng mật khẩu và thực hiện việc thu hồi chức năng này khi đã sử dụng xong;

d) Khi mở các tập tin đính kèm theo thư điện tử, nếu biết rõ người gửi thư thì phải lưu tập tin vào máy tính rồi quét virus trước khi mở, không được mở các thư điện tử có tập tin đính kèm có nguồn gốc không rõ ràng để phòng, tránh virus, phần mềm gián điệp đính kèm theo thư;

đ) Phải đặt mật khẩu truy nhập vào máy tính của mình, đồng thời thiết lập chế độ bảo vệ màn hình có sử dụng mật khẩu bảo vệ sau một khoảng thời gian nhất định không sử dụng máy tính. Khi gắn thiết bị lưu trữ vào máy tính, không được trực tiếp truy cập ngay mà phải quét virus trước;

e) Khi đặt các loại mật khẩu (*tệp tin, máy tính, thư điện tử, tài khoản phần mềm quản lý văn bản,...*) nên nhiều hơn 8 ký tự, có cả số và chữ; đồng thời các loại mật khẩu nên thay đổi sau một khoảng thời gian đưa vào sử dụng, nếu có dấu hiệu lộ phải thay đổi ngay;

f) Không cài đặt phần mềm không rõ nguồn gốc, xuất xứ; không truy cập những trang web có nội dung không lành mạnh, không mở những thư điện tử không rõ địa chỉ người gửi.

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

1. Tham mưu cho UBND tỉnh về công tác đảm bảo an toàn, an ninh thông tin trên địa bàn tỉnh và chịu trách nhiệm trước UBND tỉnh trong việc đảm bảo an toàn thông tin trong hoạt động ứng dụng CNTT của các cơ quan nhà nước thuộc 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, an ninh thông tin trong hoạt động ứng dụng CNTT 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 khi phát hiện có dấu hiệu, hành vi vi phạm an toàn, an ninh thông tin; tiến hành xử lý, xử phạt theo thẩm quyền đối với các hành vi vi phạm gây thiệt hại cho hệ thống thông tin các cơ quan nhà nước trên địa bàn tỉnh.

4. Xây dựng và triển khai các chương trình đào tạo, hội nghị tuyên truyền về an toàn, an ninh thông tin trong công tác quản lý Nhà nước trên địa bàn tỉnh.

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

6. Thường xuyên cập nhật các nguy cơ gây mất an toàn, 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.

7. Tùy theo mức độ sự cố, phối hợp với Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố mất an toàn, an ninh thông tin.

8. Phối hợp với Trung tâm Chứng thực điện tử quốc gia tổ chức triển khai ứng dụng chữ ký số cho các cơ quan nhà nước của tỉnh; hướng dẫn, khuyến khích các tổ chức, doanh nghiệp và người dân trên địa bàn tỉnh tăng cường ứng dụng chữ ký số trong giao dịch điện tử.

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 xây dựng kế hoạch, tăng cường công tác tuyên truyền, phổ biến pháp luật và chịu trách nhiệm quản lý, kiểm soát, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống thông tin gây phương hại đến an ninh quốc gia và an toàn, an ninh thông tin trong cơ quan nhà nước, các tổ chức xã hội, doanh nghiệp.

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

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.

4. Điều tra, làm rõ và xử lý các trường hợp vi phạm an toàn, an ninh thông tin theo thẩm quyền.

Điều 16. Trách nhiệm của tổ chức, doanh nghiệp, cá nhân đối với việc bảo đảm an toàn, an ninh thông tin

1. Các tổ chức, doanh nghiệp cung cấp dịch vụ hạ tầng mạng, Internet, CNTT phải thiết lập đầu mối liên lạc để phối hợp, 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.

2. Tổ chức, cá nhân tham gia cung cấp thông tin và sử dụng dịch vụ trên mạng có trách nhiệm bảo đảm an toàn, an ninh thông tin trong phạm vi hệ thống thông tin của mình; phối hợp với cơ quan quản lý nhà nước có thẩm quyền và tổ chức, cá nhân khác trong việc bảo đảm an toàn, an ninh thông tin trên mạng.

3. Thực hiện các nghĩa vụ, trách nhiệm khác theo các quy định của pháp luật.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 17. Khen thưởng và xử lý vi phạm

1. Các cơ quan, đơn vị, tổ chức, doanh nghiệp và cá nhân có thành tích xuất sắc trong việc đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng CNTT trên địa bàn tỉnh Lai Châu sẽ được xem xét khen thưởng theo quy định.

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

Điều 18. Điều khoản thi hành

1. Sở Thông tin và Truyền thông có trách nhiệm hướng dẫn triển khai thực hiện Quy định này.

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

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Đỗ Ngọc An