UỶ BAN NHÂN DÂN **TỈNH LÀO CAI**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 18 /2014/QĐ-UBND	*Lào Cai, ngày 16 tháng 6 năm 2014*

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 Lào Cai

ỦY BAN NHÂN DÂN TỈNH LÀO CAI

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

Căn cứ Luật Ban hành văn bản quy phạm pháp luật của HĐND và UBND 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 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 18/TTr-STTTT ngày 23/4/2014,

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 Lào Cai.

Điều 2. Giao Sở Thông tin và Truyền thông chủ trì, phối hợp với các sở, ban, ngành, UBND các huyện, thành phố và các đơn vị có liên quan tổ chức triển khai thực hiện quyết định này.

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

TM. ỦY BAN NHÂN DÂN TỈNH
CHỦ TỊCH

Doãn Văn Hưởng

Nơi nhận:
- Bộ Thông tin và Truyền thông;
- Văn phòng Chính phủ;
- Cục Kiểm tra VBQPPL-Bộ Tư pháp;
- TT: TU, HĐND, UBND tỉnh;
- TT Đoàn ĐBQH tỉnh;
- Như Điều 3 (QĐ);
- Sở Tư pháp; Công báo tỉnh;
- Báo Lào Cai; Đài PTHT tỉnh;
- Lãnh đạo VP UBND tỉnh;
- Lưu: VT, các CV.

UỶ BAN NHÂN DÂN **TỈNH LÀO CAI**	**CỘNG HOÀ 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 Lào Cai

(Ban hành kèm theo Quyết định số : 18 /2014/QĐ-UBND ngày 16 /6/2014 của UBND tỉnh Lào Cai)

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) của các cơ quan nhà nước, đơn vị sự nghiệp thuộc tỉnh, các đoàn thể, tổ chức chính trị - xã hội và các tổ chức, doanh nghiệp cung cấp dịch vụ hạ tầng mạng, Internet, CNTT trên địa bàn tỉnh Lào Cai.

Điều 2. Đối tượng áp dụng.

1. Quy định này áp dụng đối với các sở, ban, ngành, đơn vị sự nghiệp thuộc tỉnh; Ủy ban nhân dân (UBND) các huyện, thành phố; các đoàn thể, tổ chức chính trị - xã hội trên địa bàn tỉnh Lào Cai (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 nêu tại khoản 1 Điều này và các tổ chức, cá nhân tham gia vận hành, khai thác và sử dụng hệ thống thông tin của các cơ quan nêu tại khoản 1 Điều này.

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. *Mạng* là khái niệm chung dùng để chỉ mạng viễn thông cố định, di động, Internet và mạng máy tính.

5. *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.

6. *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.

7. *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.

8. *Thông tin số* là thông tin được tạo lập bằng phương pháp dùng tín hiệu số.

9. *Máy tính cá nhân* là máy tính để bàn (Desktop computer), máy tính xách tay (Laptop), máy tính bảng (Tablet computer) và tương đương được CBCCVC, người lao động sử dụng để thực hiện những nhiệm vụ theo chuyên môn được giao.

10. *Máy trạm* là máy tính cá nhân khi được kết nối với hệ thống mạng nội bộ của cơ quan, đơn vị.

11. *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.

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

1. 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.

2. 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.

3. 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.

4. 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 của cơ quan, tổ chức xã hội, doanh nghiệp, cá nhân, gây nguy hại, xóa, làm sai lệch thông tin trên mạng; ảnh hưởng tới hoạt động bình thường của hệ thống thông tin, khả năng truy cập hợp pháp của người sử dụng tới hệ thống thông tin trừ trường hợp pháp luật cho phép.

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

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

4. Lợi dụng mạng để truyền bá tư tưởng, văn hóa độc hại, đồi trụy, kích động, chống phá các chủ trương đường lối của Đảng, chính sách pháp luật của Nhà nước.

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 chuyên trách CNTT trực tiếp quản lý. Áp dụng các biện pháp và kiểm soát ra vào thích hợp;

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 ổn định theo quy định tại điểm b Khoản 1 Điều 6 Quy định 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 tính cá nhân:

a) Kích hoạt và thiết lập chế độ tự động cập nhật bản vá lỗ hổng bảo mật cho các phần mềm trên mỗi máy tính cá nhân; đặt mật khẩu đăng nhập, chế độ bảo vệ màn hình cho máy tính cá nhân nhằm hạn chế các nguy cơ xâm nhập trái phép;

b) Cài đặt phần mềm phòng, chống virus, mã độc cho tất cả các máy tính trong mạng nội bộ của cơ quan, đơn vị, thiết lập chế độ cập nhật hàng ngày cho phần mềm này;

c) 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,...;

d) Hạn chế sử dụng chức năng chia sẻ thư mục (Sharing). Khi sử dụng chức năng này thiết lập cơ chế chỉ đọc (Read Only) đối với những thư mục được chia sẻ trong mạng nội bộ. Chỉ sử dụng cơ chế cho phép toàn quyền đọc, ghi (Read, Write) khi thật cần thiết yêu cầu phải sử dụng mật khẩu khi truy cập thư mục chia sẻ và thực hiện thu hồi chức năng này sau khi đã sử dụng xong.

4. 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.

5. 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 và phần mềm ứng dụng CNTT.

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.

6. An toàn khi khai thác, sử dụng các phần mềm dùng chung của tỉnh:

a) Nghiêm cấm tiết lộ tài khoản đăng nhập, đấu nối, truy cập trái phép vào hệ thống các phần mềm dùng chung của tỉnh;

b) Tài khoản truy cập các phần mềm dùng chung của tỉnh phải đổi mật khẩu mặc định ngay sau khi được Sở Thông tin và Truyền thông cấp, định kỳ hàng tháng thay đổi mật khẩu, đặt mật khẩu với độ an toàn cao; không đặt chế độ ghi nhớ mật khẩu khi sử dụng,..;

c) Khi khai thác, sử dụng các phần mềm dùng chung của tỉnh tại các điểm truy cập Internet công cộng, tuyệt đối không đặt chế độ lưu trữ mật khẩu trong các trình duyệt.

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.

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

Điều 10. Trách nhiệm của các cơ quan, đơn vị.

1. Thủ trưởng các cơ quan, đơn vị có trách nhiệm tuyên truyền, nâng cao nhận thức cho CBCCVC về các nguy cơ mất an toàn, an ninh thông tin; tổ chức triển khai thực hiện đầy đủ các nội dung quy định tại Quy định này và chịu trách nhiệm trước UBND tỉnh trong công tác đảm bảo an toàn, an ninh thông tin của cơ quan, đơn vị mình.

2. Ban hành quy định nội bộ về đảm bảo an toàn, an ninh thông tin; trang bị đầy đủ các kiến thức cơ bản về máy tính, mạng máy tính, bảo mật thông tin, các quy định của pháp luật và nội quy của cơ quan về an toàn, an ninh thông tin cho CBCCVC trước khi truy nhập và sử dụng hệ thống thông tin.

3. Bố trí cán bộ chuyên trách, phụ trách về CNTT, an toàn, an ninh thông tin có đủ phẩm chất năng lực, trình độ chuyên môn để trực tiếp quản lý, vận hành hạ tầng kỹ thuật và hệ thống thông tin.

4. 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.

5. Thường xuyên tổ chức thực hiện tự kiểm tra, rà soát, 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.

6. Khuyến khích các cơ quan, đơn vị hằng năm chủ động trích một phần kinh phí thường xuyên hoặc lồng ghép đầu tư hệ thống an toàn, an ninh thông tin trong các hoạt động đầu tư ứng dụng CNTT chuyên ngành.

7. Phối hợp với Sở Thông tin và Truyền thông và các đơn vị có liên quan trong công tác xây dựng, bảo trì, nâng cấp hệ thống bảo đảm an toàn, an ninh thông tin của đơn vị.

8. Áp dụng mọi biện pháp để khắc phục và hạn chế thiệt hại do sự cố xảy ra, lập biên bản báo cáo cho cơ quan cấp trên quản lý trực tiếp, đồng thời thông báo bằng văn bản cho Sở Thông tin và Truyền thông. Trường hợp có sự cố nghiêm trọng vượt quá khả năng khắc phục của đơn vị, phải báo cáo ngay cho Sở Thông tin và Truyền thông và cơ quan quản lý nhà nước cấp trên.

9. 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.

10. Tạo điều kiện thuận lợi và cung cấp đầy đủ, chính xác, kịp thời những thông tin cần thiết cho cơ quan chức năng kiểm tra, tham gia khắc phục sự cố và thực hiện theo đúng hướng dẫn.

11. 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 20 tháng 11 hằng năm).

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

1. Trách nhiệm của cán bộ chuyên trách, phụ trách CNTT:

a) Chịu trách nhiệm xây dựng, triển khai các biện pháp quản lý vận hành, quản lý kỹ thuật, xây dựng phương án hạn chế, khắc phục các rủi ro và nguy cơ có thể xảy ra, tham mưu xây dựng quy định về đảm bảo an toàn cho hệ thống thông tin của cơ quan, đơn vị theo Quy định này và các quy định có liên quan khác của Nhà nước;

b) Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm tra, phát hiện và khắc phục các sự cố mất an toàn, an ninh thông tin tại cơ quan, đơn vị mình;

c) Trực tiếp thiết lập các biện pháp kỹ thuật đảm bảo an toàn cho các máy tính cá nhân trong cơ quan, đơn vị mình; hướng dẫn các CBCCVC của cơ quan, đơn vị tuân thủ các biện pháp đảm bảo an toàn, an ninh thông tin trong khai thác, sử dụng phần mềm và các trang thiết bị CNTT;

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

2. Trách nhiệm của CBCCVC:

a) Thường xuyên cập nhật và chấp hành nghiêm túc những chính sách, các quy định về an toàn, an ninh thông tin theo Quy định này và của cơ quan, đơn vị cũng như các quy định khác của pháp luật. Nâng cao ý thức cảnh giác và trách nhiệm đảm bảo an toàn,

an ninh thông tin tại cơ quan, đơn vị. Thực hiện những hướng dẫn về an toàn, an ninh thông tin của cán bộ chuyên trách, phụ trách CNTT;

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

c) Tham gia đầy đủ các chương trình đào tạo, hội nghị về an toàn, an ninh thông tin do Sở Thông tin và Truyền thông hoặc các đơn vị chuyên môn tổ chức.

Điều 12. 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 Ban cơ yếu Chính phủ 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 13. 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 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. Tăng cường công tác phòng ngừa, phát hiện, tuyên truyền, phổ biến pháp luật về bảo vệ bí mật nhà nước, về phòng, chống, phát hiện tội phạm trong việc đảm bảo an toàn, an ninh thông tin.

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

4. Điều tra, làm rõ các trường hợp vi phạm an toàn, an ninh thông tin và xử lý theo đúng quy định của pháp luật.

Điều 14. 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 15. Khen thưởng và xử lý vi phạm.

1. Các cơ quan, đơn vị, tổ chức, doanh nhiệp và các 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 Lào Cai sẽ được xem xét khen thưởng theo quy định.

2. Các cơ quan, đơn vị, 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 16. 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 TỈNH
CHỦ TỊCH

Doãn Văn Hưởng