TỈNH ỦY BÌNH THUẬN	**ĐẢNG CỘNG SẢN VIỆT NAM**
*	
Số 1596 -QĐ/TU	*Phan Thiết, ngày 27 tháng 01 năm 2015*

QUYẾT ĐỊNH

về việc 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 Đảng, Ủy ban Mặt trận Tổ quốc Việt Nam và các đoàn thể chính trị – xã hội tỉnh.

- Căn cứ Quyết định số 1381-QĐ/TU, ngày 05 tháng 8 năm 2014 về việc ban hành Quy chế làm việc của Ban Chấp hành Đảng bộ tỉnh khóa XII, nhiệm kỳ 2010 – 2015 (sửa đổi, bổ sung);

- Căn cứ Luật Công nghệ thông tin số 67/2006/QH11, ngày 29 tháng 6 năm 2006 của Quốc hội;

- Căn cứ Luật Giao dịch Điện tử số 51/2005/QH11, ngày 29 tháng 11 năm 2005 của Quốc hội;

- Căn cứ Nghị định số 33/2002/NĐ-CP, ngày 28 tháng 3 năm 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 tháng 4 năm 2007 của Chính phủ quy định về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

- Căn cứ Quyết định số 63/QĐ-TTg, ngày 13 tháng 01 năm 2010 của Thủ tướng Chính phủ về việc phê duyệt Quy hoạch phát triển an toàn thông tin số quốc gia đến năm 2020;

- Căn cứ Thông tư số 23/2011/TT-BTTTT, ngày 11 tháng 8 năm 2011 của Bộ Thông tin và Truyền thông Quy định về việc quản lý, vận hành, sử dụng và bảo đảm an toàn thông tin trên Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;

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

- Căn cứ Chỉ thị số 28-CT/TW, ngày 16 tháng 9 năm 2013 của Ban Bí thư

Số hóa bởi Văn phòng Tỉnh ủy Bình Thuận. http://binhthuancpv.org.vn/

Trung ương Đảng về tăng cường công tác bảo đảm an toàn thông tin mạng;

- Căn cứ Chương trình hành động số 23-NQ/TU, ngày 30 tháng 10 năm 2013 của Ban Thường vụ Tỉnh ủy (khóa XII) thực hiện Chỉ thị số 28-CT/TW, ngày 16 tháng 9 năm 2013 của Ban Bí thư Trung ương Đảng về tăng cường công tác bảo đảm an toàn thông tin mạng;

- Theo đề nghị của Ban Chỉ đạo công nghệ thông tin khối Đảng tỉnh;

BAN THƯỜNG VỤ TỈNH ỦY 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 Đảng, Ủy ban Mặt trận Tổ quốc Việt Nam và các đoàn thể chính trị – xã hội tỉnh*".

Điều 2. Quyết định này thay thế Quyết định số 656-QĐ/TU, ngày 31 tháng 7 năm 2012 của Ban Thường vụ Tỉnh ủy về việc 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 Đảng, Ủy ban Mặt trận Tổ quốc Việt Nam và các đoàn thể chính trị – xã hội tỉnh; và có hiệu lực kể từ ngày ký.

Điều 3. Văn phòng Tỉnh uỷ, các Ban của Tỉnh uỷ, Ban Bảo vệ chăm sóc sức khỏe cán bộ tỉnh, các huyện, thị, thành uỷ, đảng uỷ trực thuộc, Ủy ban Mặt trận Tổ quốc Việt Nam và các đoàn thể chính trị – xã hội tỉnh chịu trách nhiệm thực hiện Quyết định này./.

Nơi nhận:
- Như điều 3;
- Lưu Văn phòng Tỉnh ủy.

T/M BAN THƯỜNG VỤ
PHÓ BÍ THƯ

(đã ký, đóng dấu)

Nguyễn Mạnh Hùng

QUY ĐỊNH

đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan Đảng, Ủy ban Mặt trận Tổ quốc Việt Nam và các đoàn thể chính trị – xã hội tỉnh

(Ban hành kèm theo Quyết định số 1596-QĐ/TU, ngày 27 tháng 01 năm 2015 của Ban Thường vụ Tỉnh ủy)

Chương I

QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy định này quy định các nội dung đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin (CNTT) của các cơ quan Đảng, Ủy ban Mặt trận Tổ quốc Việt Nam và các đoàn thể chính trị – xã hội tỉnh bao gồm: Công tác xây dựng các quy định quản lý đảm bảo an toàn, an ninh thông tin; công tác bảo vệ bí mật nhà nước; việc áp dụng các biện pháp quản lý kỹ thuật, quản lý vận hành đảm bảo an toàn, an ninh thông tin đối với hệ thống thông tin.

Điều 2. Đối tượng áp dụng

1. Quy định này áp dụng đối với các huyện, thị, thành ủy, đảng ủy trực thuộc, các ban của Tỉnh ủy, Văn phòng Tỉnh ủy, Ban Bảo vệ chăm sóc sức khỏe cán bộ tỉnh, Ủy ban Mặt trận Tổ quốc Việt Nam và các đoàn thể chính trị – xã hội tỉnh (*sau đây gọi tắt là các cơ quan, đơn vị*).

2. Cán bộ, công chức, viên chức và người lao động đang làm việc trong các cơ quan, đơn vị nêu tại Khoản 1 điều này và những cá nhân, tổ chức 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.

Điều 3. Giải thích từ ngữ

1. 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, tri thức nhằm phục vụ cho các mục tiêu của tổ chức.

2. An toàn thông tin: Là sự bảo vệ thông tin và các hệ thống thông tin được an toàn, tránh bị truy cập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính sẵn sàng của thông tin.

3. An ninh thông tin: Là việc đảm bảo 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.

4. Tính tin cậy: Là đảm bảo thông tin chỉ có thể được truy cập bởi những người được cấp quyền truy cập.

5. Tính toàn vẹn: Là bảo vệ tính chính xác, tính đầy đủ của thông tin và các phương pháp xử lý thông tin.

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

7. Môi trường mạng bao gồm: Mạng nội bộ (LAN); mạng diện rộng của Đảng (WAN); mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước; mạng riêng ảo (VPN), mạng Intranet; mạng Internet.

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

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

Chương II

QUY ĐỊNH ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 4. Nguyên tắc đảm bảo 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 hệ thống thông tin của cơ quan, đơn vị.

2. 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 với các tiêu chuẩn, quy chuẩn kỹ thuật theo quy định.

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

Điều 5. Các hành vi bị nghiêm cấm

1. Ngăn chặn trái phép việc truy cập, truyền tải thông tin trên mạng.

2. Tạo, cài đặt, phát tán phần mềm độc hại, virus máy tính; xâm nhập trái phép, chiếm quyền điều khiển hệ thống thông tin, sửa đổi, xóa, làm sai lệch thông tin trên mạng, tạo lập công cụ tấn công trên mạng.

3. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

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

Điều 6. Những quy định đảm bảo 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 cán bộ, công chức, viên chức, người lao động trước khi tham gia sử dụng hệ thống thông tin.

2. Bố trí người làm công tác chuyên trách về công nghệ thông tin phải có chuyên ngành phù hợp và được đào tạo, bồi dưỡng chuyên môn đối với lĩnh vực an toàn, an ninh thông tin.

3. Quan tâm kinh phí cho hạng mục về an toàn, an ninh thông tin.

4. Các cơ quan, đơn vị căn cứ vào các nội dung của tiêu chuẩn TCVN 7562:2005 và TCVN ISO/IEC 27001:2009 để xây dựng, ban hành quy chế nội bộ đảm bảo an toàn, an ninh thông tin.

Điều 7. Quản lý, vận hành hệ thống thông tin của đơn vị

1. Hệ thống thông tin của các cơ quan, đơn vị phải có cơ chế cân bằng tải, sao lưu (backup) dữ liệu ở mức 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 đảm bảo yêu cầu kỹ thuật; dữ liệu được sao lưu phải đảm bảo 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 cơ quan, đơn vị phải được triển khai cơ chế bảo mật và an toàn thông tin bằng các thiết bị phần cứng và phần mềm:

- Đầu tư trang bị các thiết bị phần cứng, phần mềm về bảo mật như tường lửa (firewall), thiết bị phát hiện, phòng, chống xâm nhập trái phép (IDS/IPS), hệ thống an toàn dữ liệu (tủ/băng đĩa/SAN/NAS...) và tổ chức mô hình mạng hợp lý, phù hợp với quy mô hệ thống thông tin của cơ quan, đơn vị .

- Sử dụng phần mềm chống vi-rút (virus) máy tính có bản quyền trên các thiết bị mạng và máy tính quan trọng chứa nhiều dữ liệu, phần mềm ứng dụng của đơn vị như: máy chủ (server), máy tính chứa dữ liệu tập trung,…

3. Hệ thống thông tin của cơ quan, đơn vị (tùy theo quy mô) phải có chức

năng giám sát truy cập từ ngoài vào hệ thống, từ hệ thống gửi ra bên ngoài; ghi lại nhật ký (log file) ra, vào hệ thống để phục vụ công tác khắc phục sự cố, điều tra, phân tích và làm rõ các nguy cơ gây ra mất an toàn, an ninh thông tin; chức năng không cho người dùng truy cập một số website không phù hợp với quy định hiện hành.

4. Hệ thống mạng không dây (wireless) của các cơ quan, đơn vị phải được thiết lập khóa khi truy cập.

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.

6. 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 (password) phức tạp (trên 8 ký tự và bao gồm: Ký tự hoa, ký tự thường, ký tự đặc biệt và chữ số); mật khẩu phải định kỳ thay đổi với tần suất tối thiểu 02 tháng/lần; 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.

7. Đảm bảo an toàn cho máy tính cá nhân:

a. Tài khoản đăng nhập máy tính phải được thiết lập mật khẩu; khi sử dụng máy tính hạn chế việc sử dụng chức năng chia sẻ tài nguyên (sharing) qua môi trường mạng, nếu có sử dụng chức năng này cần thiết lập thuộc tính bảo mật bằng mật khẩu, phân quyền và thực hiện việc thu hồi chức năng này khi đã sử dụng xong.

b. Các máy tính khi không sử dụng trong thời gian dài (quá 4 giờ làm việc) cần tắt máy hoặc ngưng kết nối mạng, để tránh bị các tin tặc (hacker) lợi dụng, sử dụng chức năng điều khiển từ xa để tấn công vào các hệ thống thông tin của cơ quan, đơn vị.

c. Chỉ được mở các tập tin đính kèm trong thư điện tử khi biết rõ nguồn gốc người gửi thư; không được mở các thư điện tử có tập tin đính kèm không rõ nguồn gốc người gửi để tránh trường hợp có thể virus, phần mềm gián điệp... được đính kèm theo thư và lây nhiễm vào máy tính.

d. Tài khoản đăng nhập Trang Thông tin điện tử của Tỉnh ủy trên Internet phải được thiết lập mật khẩu phức tạp (trên 8 ký tự và bao gồm: ký tự hoa, ký tự thường, ký tự đặc biệt và chữ số) và định kỳ thay đổi với tần suất tối thiểu 01

lần/tháng.

8. Đảm bảo an toàn cho các máy chủ:

a. Tài khoản đăng nhập máy chủ phải được thiết lập mật khẩu theo quy định tại Khoản 6, Điều 7 của Quy định này.

b. Đóng tất cả các cổng (Port) dịch vụ khi không sử dụng; thiết lập chế độ tự động cập nhật bản vá lỗ hổng bảo mật cho phần mềm hệ điều hành, phần mềm cơ sở dữ liệu... được cài đặt trên các máy chủ.

c. Khi kết nối từ xa, nhất là từ Internet vào máy chủ để quản trị, cài đặt phải sử dụng phương thức kết nối có mã hóa như SSH, VPN…

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, nhận dạng virus, mã độc mới.

9. Đảm bảo an toàn khi khai thác, sử dụng các phần mềm dùng chung trên mạng diện rộng của Đảng:

a. Nghiêm cấm tiết lộ tài khoản đăng nhập, đấu nối, truy cập trái phép vào các phần mềm dùng chung trên mạng diện rộng của Đảng; không đặt chế độ ghi nhớ mật khẩu khi sử dụng.

b. Tuyệt đối không đặt chế độ lưu trữ mật khẩu trong các trình duyệt khi truy cập, khai thác, sử dụng Trang thông tin điện tử của Tỉnh ủy (gọi tắt là website).

10. Đảm bảo an toàn cho website:

a. Phải tổ chức mô hình website hợp lý; cài đặt các hệ thống phòng thủ quan trọng như tường lửa (Firewall), thiết bị phát hiện/phòng, chống xâm nhập (IDS/IPS), tường lửa mức ứng dụng web (Web Application Firewall).

b. Định kỳ cần phải đánh giá, kiểm định nhằm tránh các lỗi bảo mật thường xuyên xảy ra trên ứng dụng web như: SQL Injection, Cross Site Scripting (XSS)...

c. Phải thiết lập cơ chế sao lưu định kỳ một cách tự động nhằm đảm bảo việc sao lưu đầy đủ các dữ liệu theo yêu cầu; áp dụng chính sách ghi, lưu tập trung biên bản hoạt động (log file) cần thiết để phục vụ công tác điều tra, khắc phục khi xảy ra sự cố.

11. Sử dụng các thiết bị lưu trữ (USB, ổ cứng gắn ngoài,...) an toàn, đúng cách để phòng ngừa virus, phần mềm gián điệp xâm nhập máy tính: khi gắn thiết

bị lưu trữ vào máy tính, không được trực tiếp truy cập ngay mà phải quét virus trước khi sử dụng; thực hiện việc đánh số, dán nhãn để tránh nhầm lẫn nhằm phục vụ cho công tác phục hồi dữ liệu một cách nhanh nhất.

Điều 8. Bảo vệ bí mật nhà nước trong công tác ứng dụng công nghệ thông tin

1. Không được sử dụng thiết bị (máy tính để bàn, máy tính xách tay, máy tính bảng, điện thoại thông minh...) có kết nối mạng để soạn thảo văn bản, lưu trữ thông tin có nội dung thuộc bí mật nhà nước; không cung cấp tin, tài liệu và đưa thông tin bí mật nhà nước trên mạng.

2. Không bật các thiết bị kết nối mạng trong các cuộc họp có nội dung bí mật nhà nước.

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

4. Khi sửa chữa, khắc phục các sự cố của máy tính dùng để soạn thảo văn bản mật phải có sự giám sát, quản lý chặt chẽ của cán bộ có thẩm quyền.

5. Đối với các thiết bị công nghệ thông tin, viễn thông,... được sử dụng để lưu trữ và truyền thông tin bí mật nhà nước phải được kiểm định của cơ quan chức năng trước khi đưa vào sử dụng.

6. 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. Các thiết bị lưu trữ không sử dụng tiếp cho công việc của cơ quan, đơn vị (thanh lý, cho, tặng) phải được xóa nội dung bằng phần mềm hoặc bằng thiết bị hủy dữ liệu chuyên dụng, đảm bảo không phục hồi được dữ liệu.

Điều 9. Cán bộ chuyên trách về công nghệ thông tin của cơ quan, đơn vị

1. Phải đảm bảo điều kiện được đào tạo, bồi dưỡng, học tập, nghiên cứu, tiếp thu kiến thức, kỹ thuật và công nghệ 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 cơ quan, 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 trong toàn hệ thống; triển khai các giải pháp kỹ thuật 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. Cấu hình hệ thống với những chính sách bảo mật phù hợp hoạt động của hệ thống thông tin cơ quan, đơn vị; đồng thời xác định các chức năng, cổng giao tiếp (port), giao thức (protocol) và dịch vụ (service) mạng không cần thiết để cấm hoặc hạn chế sử dụng.

7. Thường xuyên sao lưu dữ liệu theo quy định; kiểm tra dữ liệu sao lưu phải đảm bảo tính sẵn sàng và toàn vẹn.

8. Sử dụng công cụ hỗ trợ để kiểm tra, giám sát dữ liệu, thông tin từ bên trong hệ thống thông tin gửi ra bên ngoài khi cần thiết.

9. Thực hiện thu hồi và vô hiệu hóa sử dụng tất cả các tài khoản, thiết bị thẻ dùng để truy cập vào hệ thống thông tin của cán bộ, công chức, viên chức ngay sau khi không còn làm việc tại cơ quan, đơn vị.

10. 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 cơ quan, đơn vị; nguyên nhân gây ra các rủi ro và nguy cơ gây mất an toàn, an ninh thông tin 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 xảy ra.

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

1. Đối với người sử dụng:

a. Thông tin, báo cáo kịp thời cho cán bộ chuyên 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 trong quá trình tham gia vào hệ thống thông tin của cơ quan, đơn vị.

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

2. Đối với cán bộ chuyên trách về công nghệ thông tin:

a. Mở sổ theo dõi và 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).

b. Khẩn trương triển khai các biện pháp kỹ thuật để giải quyết và khắc phục sự cố; đồng thời báo cáo sự cố và kết quả khắc phục sự cố cho Lãnh đạo cơ quan, đơn vị.

c. Trong trường hợp sự cố xảy ra ngoài khả năng giải quyết của cơ quan, đơn vị phải kịp thời báo cáo cho Phòng Cơ yếu - Công nghệ thông tin, Văn phòng Tỉnh ủy để được hỗ trợ, hướng dẫn và phối hợp khắc phục sự cố.

3. Văn phòng Tỉnh ủy:

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

b. Chỉ đạo Phòng Cơ yếu - Công nghệ thông tin 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 cơ quan có liên quan làm rõ các nguyên nhân gây ra sự cố mất an toàn, an ninh thông tin khi có ý kiến chỉ đạo của Thường trực Tỉnh ủy.

Chương III

TRÁCH NHIỆM ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

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

1. Lãnh đạo các cơ quan, đơn vị chịu trách nhiệm toàn diện trước Ban Thường vụ Tỉnh ủy trong công tác đảm bảo an toàn, an ninh thông tin đối với toàn bộ hệ thống thông tin của cơ quan, đơn vị mình.

2. Thực hiện và chỉ đạo cán bộ, công chức, viên chức thực hiện nghiêm túc Quy định này.

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

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. Khi có sự cố hoặc nguy cơ mất an toàn, an ninh thông tin 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 cơ quan, đơn vị mình, đồng thời lập biên bản và báo cáo bằng văn bản cho cơ quan có liên quan.

6. Bố trí máy tính riêng, không kết nối mạng Internet để soạn thảo văn bản, lưu trữ thông tin có nội dung mật theo quy định.

7. Xây dựng, triển khai kế hoạch đảm bảo an toàn, an ninh thông tin và tổng hợp báo cáo về Ban Chỉ đạo CNTT khối đảng theo định kỳ hàng năm.

Điều 12. Trách nhiệm của Văn phòng Tỉnh ủy

1. Chịu trách nhiệm trước Ban Thường vụ Tỉnh ủy về công tác đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan, đơn vị.

2. Tham mưu Ban Thường vụ Tỉnh ủy ban hành:

a. Văn bản chỉ đạo, kế hoạch, đề án nhằm đảm bảo an toàn, an ninh 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.

3. Hàng năm phối hợp với các tổ chức có liên quan đào tạo chuyên sâu về an toàn, an ninh thông tin cho cán bộ chuyên trách công nghệ thông tin của các cơ quan, đơn vị.

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

5. Tổ chức Hội nghị, Hội thảo chuyên đề về an toàn, an ninh thông tin.

6. Phối hợp với các đơn vị có liên quan trong thực hiện nhiệm vụ đảm bảo an toàn, an ninh thông tin.

7. Hướng dẫn các cơ quan, đơn vị xây dựng quy chế nội bộ, hỗ trợ kỹ thuật, nội dung, thời gian báo cáo công tác đảm bảo an toàn, an ninh thông tin.

8. Tổng hợp báo cáo và thông báo về tình hình an toàn, an ninh thông tin theo định kỳ cho Ban Thường vụ Tỉnh ủy và các cơ quan, đơn vị có liên quan.

9. Phối hợp với Ban Cơ yếu Chính phủ, Sở Thông tin và Truyền thông để thực hiện việc ứng dụng chữ ký số trong các cơ quan Đảng, Ủy ban Mặt trận Tổ quốc Việt Nam và các đoàn thể chính trị tỉnh.

10. Phối hợp với các cơ quan, đơn vị có liên quan thành lập Tổ Ứng cứu sự cố mạng máy tính trong các cơ quan Đảng, Ủy ban Mặt trận Tổ quốc Việt Nam và các đoàn thể chính trị - xã hội tỉnh.

Điều 13. Trách nhiệm của cán bộ, công chức và viên chức

1. Trách nhiệm của cán bộ chuyên trách công nghệ thông tin tại cơ quan, đơn vị:

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 đảm bảo an toàn, an ninh thông tin cho toàn bộ hệ thống thông tin của cơ quan, đơn vị mình đúng theo nội dung quy định 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 Phòng Cơ yếu - Công nghệ thông tin, Văn phòng Tỉnh ủy trong quá trình khắc phục sự cố về an toàn, an ninh thông tin.

2. Trách nhiệm của cán bộ, công chức, viên chức tham gia sử dụng và khai thác hệ thống thông tin tại cơ quan, đơn vị:

a. Nghiêm chỉnh thực hiện các quy định, quy chế, quy trình nội bộ về đảm bảo an toàn, an ninh thông tin của cơ quan, đơn vị cũng như các quy định khác của pháp luật về nội dung này.

b. Khi phát hiện nguy cơ hoặc sự cố mất an toàn, an ninh thông tin phải báo cáo kịp thời cho cán bộ chuyên trách công nghệ thông tin của cơ quan, 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.

d. Không sử dụng mạng xã hội như: Google Plus+, MySpace, LinkedIn, Twitter, Facebook,..., blog cá nhân để đăng tải, phát tán, truyền tải lại những nội dung phản động, tuyên truyền, xuyên tạc, đả kích Đảng và Nhà nước.

đ. Không sử dụng các hộp thư điện tử miễn phí Gmail, Yahoo,... trong hoạt động công vụ và tại máy tính có nối mạng ở cơ quan nhằm bảo đảm bảo mật, an toàn thông tin trên môi trường mạng.

e. Cán bộ, công chức, viên chức, người lao động sử dụng các thiết bị lưu trữ dữ liệu di động (máy tính xách tay, thiết bị số cầm tay, thẻ nhớ USB, ổ cứng di động, băng từ...) để lưu thông tin thuộc danh mục bí mật nhà nước có trách nhiệm bảo vệ các thiết bị này và thông tin trên thiết bị, tránh làm mất, lộ thông tin. Nghiêm cấm việc bán, cho mượn, giao người không có trách nhiệm sử dụng thiết bị do cá nhân tự trang bị có lưu giữ bí mật Nhà nước.

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

Điều 14. Kiểm tra định kỳ và đột xuất

1. Định kỳ hàng năm, các cơ quan, đơn vị tự thực hiện kiểm tra và có báo cáo kết quả về công tác đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan, đơn vị về Ban Chỉ đạo CNTT khối đảng.

2. Trong trường hợp cần thiết, Ban chỉ đạo CNTT khối đảng xây dựng kế hoạch và trình Ban Thường vụ Tỉnh ủy thành lập Đoàn kiểm tra.

Điều 15. Trách nhiệm và phối hợp trong công tác kiểm tra

1. Đoàn kiểm tra có trách nhiệm thông báo thời gian, địa điểm, nội dung và thành phần cho cơ quan, đơn vị được kiểm tra biết trước ít nhất 03 ngày để chuẩn bị.

2. Cơ quan, đơn vị được kiểm tra:

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

b. Có đại diện lãnh đạo, các thành viên Tổ công nghệ thông tin và cán bộ chuyên trách công nghệ thông tin của cơ quan, đơn vị để cùng làm việc với Đoàn kiểm tra.

c. Tạo thuận lợi cho công tác kiểm tra.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 16. Trách nhiệm của Ban Chỉ đạo CNTT khối Đảng

1. Tổng hợp báo cáo công tác đảm bảo an toàn, an ninh thông tin của các cơ quan, đơn vị; đề xuất khen thưởng các cá nhân, đơn vị có thành tích xuất sắc theo quy định.

2. Tham mưu điều chỉnh, bổ sung kịp thời các tiêu chuẩn đánh giá mức độ an toàn, an ninh thông tin đối với hệ thống thông tin của các cơ quan, đơn vị phù hợp với sự phát triển về công nghệ, yêu cầu của từng giai đoạn phát triển và nhiệm vụ chuyên môn của các cơ quan, đơn vị.

Điều 17. Các cơ quan, đơn vị

1. Tăng cường công tác phòng ngừa, phát hiện và 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.

2. Phối hợp với các cơ quan chức năng kiểm tra an ninh, an toàn thiết bị điện tử trước khi đưa vào sử dụng tại các bộ phận quan trọng, cơ mật, nơi chứa đựng bí mật của cơ quan, đơn vị.

3. Xây dựng kế hoạch cụ thể hóa thực hiện Quy định này. Định kỳ báo cáo kết quả thực hiện về Ban chỉ đạo CNTT khối Đảng./.