ỦY BAN NHÂN DÂN TỈNH BẾN TRE	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 47 /2023/QĐ-UBND	*Bến Tre, ngày 14 tháng 12 năm 2023*

QUYẾT ĐỊNH

Ban hành Quy chế đảm bảo an toàn, an ninh thông tin trên môi trường mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Bến Tre

ỦY BAN NHÂN DÂN TỈNH BẾN TRE

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19 tháng 6 năm 2015;

Căn cứ Luật sửa đổi, bổ sung một số điều Luật Tổ chức Chính phủ và Luật Tổ chức chính quyền địa phương ngày 22 tháng 11 năm 2019;

Căn cứ Luật Ban hành văn bản quy phạm pháp luật ngày 22 tháng 6 năm 2015;

Căn cứ Luật sửa đổi, bổ sung một số điều của Luật Ban hành văn bản quy phạm pháp luật ngày 18 tháng 6 năm 2020;

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

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

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan 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 Nghị định số 27/2018/NĐ-CP ngày 01 tháng 3 năm 2018 sửa đổi, bổ sung một số điều của 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 Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 142/2016/NĐ-CP ngày 14 tháng 10 năm 2016 của Chính phủ về ngăn chặn xung đột thông tin trên mạng;

Căn cứ Nghị định số 53/2022/NĐ-CP ngày 15 tháng 8 năm 2022 của Chính phủ về việc quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Nghị định số 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 của Chính phủ về bảo vệ dữ liệu cá nhân;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị

định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 2533/TTr-STTTT ngày 12 tháng 12 năm 2023.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn, an ninh thông tin trên môi trường mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Bến Tre.

Điều 2. Điều khoản thi hành

1. Chánh Văn phòng Ủy ban nhân dân tỉnh, Giám đốc Sở Thông tin và Truyền thông, Thủ trưởng các sở, ban, ngành, Chủ tịch Ủy ban nhân dân các huyện, thành phố và các tổ chức, cá nhân có liên quan căn cứ Quyết định thi hành.

2. Quyết định này có hiệu lực kể từ ngày 29 tháng 12 năm 2023 và thay thế Quyết định số 22/2013/QĐ-UBND ngày 08 tháng 8 năm 2013 của Ủy ban nhân dân tỉnh ban hành Quy chế đảm bảo an toàn, an ninh thông tin trên môi trường mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Bến Tre./.

Nơi nhận:
- Như Điều 2;
- Văn phòng Chính phủ;
- Bộ Thông tin và Truyền thông;
- Cục Kiểm tra văn bản QPPL - Bộ Tư pháp;
- TT.TU, TT.HĐND tỉnh;
- Chủ tịch, các PCT.UBND tỉnh;
- Văn phòng Tỉnh ủy, các Ban đảng;
- Đoàn ĐBQH tỉnh;
- UBMTTQ và các tổ chức CT-XH tỉnh;
- Sở Tư pháp;
- Các Sở, ban, ngành tỉnh;
- Chánh, PCVP.UBND tỉnh;
- Báo ĐK, Đài PTTH tỉnh;
- UBND các huyện, thành phố;
- UBND các xã, phường, thị trấn;
- Phòng: KGVX, TH, Cổng TTĐT;
- Lưu: VT, Ph.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Trần Ngọc Tam

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

QUY CHẾ

Đảm bảo an toàn, an ninh thông tin trên môi trường mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Bến Tre

(Kèm theo Quyết định số 47 /2023/QĐ-UBND ngày 14 tháng 12 năm 2023 của Ủy ban nhân dân tỉnh Bến Tre)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định các nội dung về đảm bảo an toàn, an ninh thông tin trên môi trường mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Bến Tre.

Điều 2. Đối tượng áp dụng

1. Các sở, ban, ngành tỉnh; các đơn vị sự nghiệp công lập trực thuộc Ủy ban nhân dân tỉnh; Ủy ban nhân dân các huyện, thành phố; Ủy ban nhân dân các xã, phường, thị trấn; các cơ quan được ngân sách nhà nước bảo đảm kinh phí hoạt động có sử dụng các hệ thống thông tin của tỉnh (gọi tắt là cơ quan, đơn vị).

2. Cán bộ, công chức, viên chức, người lao động (gọi tắt là cán bộ, công chức, viên chức) và các cá nhân, tổ chức có liên quan tham gia vận hành, khai thác các hệ thống thông tin tại các cơ quan, đơn vị quy định tại khoản 1 Điều này.

3. Các doanh nghiệp cung cấp dịch vụ viễn thông, công nghệ thông tin, Internet; các doanh nghiệp, tổ chức, cá nhân có tham gia vào các hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của các cơ quan, đơn vị thuộc khoản 1 Điều này.

4. Khuyến khích các cơ quan, đơn vị khác hoạt động ứng dụng và phát triển công nghệ thông tin trên địa bàn tỉnh áp dụng quy chế này.

Điều 3. Nguyên tắc bảo đảm an toàn thông tin mạng

1. Bảo đảm an toàn thông tin mạng là yêu cầu bắt buộc, có tính xuyên suốt và phải thường xuyên, liên tục được nâng cao, cải tiến trong quá trình:

a) Thu thập, tạo lập, xử lý, truyền tải, lưu trữ và sử dụng thông tin, dữ liệu.

b) Thiết kế, xây dựng, vận hành, nâng cấp hoặc hủy bỏ hệ thống thông tin.

2. Cơ quan, tổ chức, cá nhân có trách nhiệm bảo đảm an toàn thông tin mạng. Hoạt động an toàn thông tin mạng của cơ quan, tổ chức, cá nhân phải đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước.

3. Công tác đảm bảo an toàn thông tin mạng phải được thực hiện trên cơ sở có sự phối hợp chặt chẽ giữa các cơ quan, đơn vị và cá nhân.

4. Xử lý sự cố an toàn thông tin phải phù hợp với trách nhiệm, quyền hạn và bảo đảm lợi ích hợp pháp của cơ quan, đơn vị và theo quy định của pháp luật.

Chương II
NỘI DUNG BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 4. Những quy định bảo đảm an toàn thông tin mạng

1. Các cơ quan, đơn vị phải phổ biến những kiến thức cơ bản về an toàn thông tin mạng cho cán bộ, công chức, viên chức trước khi tham gia sử dụng hệ thống thông tin mạng.

2. Các cơ quan, đơn vị bố trí công chức, viên chức thực hiện nhiệm vụ hoặc chuyên trách về công nghệ thông tin phải có chuyên ngành phù hợp hoặc tương đương và được đào tạo, bồi dưỡng chuyên môn đối với lĩnh vực an toàn thông tin mạng.

3. Xác định và ưu tiên phân bổ kinh phí cho các hoạt động chuyển đổi số, ứng dụng công nghệ thông tin của các cơ quan, đơn vị cho hạng mục về an toàn thông tin mạng.

4. Cán bộ, công chức, viên chức tham gia đoàn kiểm tra công tác bảo đảm an toàn thông tin mạng phải được trang bị đầy đủ những kiến thức và được tập huấn về công tác bảo đảm an toàn thông tin mạng.

Điều 5. Bảo đảm an toàn thông tin mạng các hệ thống thông tin và máy chủ

1. Các hoạt động liên quan đến xây dựng, thiết lập, nâng cấp, mở rộng, quản lý, vận hành hệ thống thông tin phải thực hiện xác định cấp độ và phương án bảo đảm an toàn thông tin mạng theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ (sau đây viết tắt là Nghị định số 85/2016/NĐ-CP); Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ (sau đây viết tắt là Thông tư số 12/2022/TT-BTTTT).

2. Quản lý, xác định hệ thống thông tin và cấp độ an toàn hệ thống thông tin; thực hiện các yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ; thực hiện kiểm tra, đánh giá an toàn thông tin mạng; tiếp nhận và thẩm định hồ sơ đề xuất cấp độ; báo cáo, chia sẻ thông tin thực hiện theo hướng dẫn của Bộ Thông tin và Truyền thông tại Thông tư số 12/2022/TT-BTTTT.

3. Các cơ quan, đơn vị chủ quản hệ thống thông tin phải tổ chức kiểm tra,

đánh giá định kỳ về an toàn thông tin mạng của các hệ thống thông tin đang quản lý. Đảm bảo an toàn thông tin mạng cho các hệ thống thông tin theo quy định tại Quyết định số 33/2023/QĐ-UBND ngày 22 tháng 8 năm 2023 của Ủy ban nhân dân tỉnh về ban hành Quy chế quản lý, khai thác và vận hành Trung tâm Giám sát An ninh mạng (SOC) tỉnh Bến Tre.

4. Bảo đảm an toàn mạng

a) Phòng đặt thiết bị công nghệ thông tin (đối với các cơ quan, đơn vị đang quản lý, vận hành các hệ thống thông tin, cơ sở dữ liệu ngành của tỉnh) phải đảm bảo các điều kiện đáp ứng các yêu cầu cơ bản (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 nguồn điện dự phòng; có bình chữa cháy hoặc hệ thống tự động cảnh báo, chữa cháy khẩn cấp; phòng, chống sét; có nội quy, quy trình làm việc trong khu vực an toàn bảo mật).

b) 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 hoặc IPS); tổ chức mô hình mạng hợp lý, phù hợp với quy mô hệ thống thông tin của cơ quan, đơn vị; cung cấp những chức năng cơ bản cho người dùng; thiết lập các chế độ phân quyền truy cập theo chỉ đạo của Thủ trưởng đơn vị.

c) Hệ thống thông tin của cơ quan, đơn vị phải được triển khai nhiều cơ chế giám sát truy cập từ ngoài vào hệ thống, từ hệ thống gửi ra bên ngoài; ghi lại nhật ký (logfile) ra vào hệ thống để phục vụ công tác khắc phục sự cố, điều tra, phân tích và làm rõ các nguy cơ gây mất an toàn thông tin mạng; Kiểm soát và theo dõi tất cả các phương pháp truy cập từ xa tới hệ thống thông tin, phát hiện sớm việc truy cập trái phép vào mạng máy tính hay thiết bị lưu trữ dữ liệu; Ghi nhận đầy đủ các thông tin trong các bản ghi nhật ký, thời gian lưu trữ các bản ghi nhật ký hệ thống tối thiểu 01 năm.

d) Hệ thống thông tin giới hạn tối đa 05 (năm) lần đăng nhập liên tiếp sai tài khoản người dùng, hệ thống tự động khóa tài khoản hoặc cô lập tài khoản trong một khoảng thời gian nhất định (tối thiểu 24 giờ), để được đăng nhập hệ thống thông tin lần kế tiếp.

đ) Cập nhật và lưu trữ cấu hình chuẩn các thành phần của hệ thống, trước khi tiến hành cài đặt, thiết lập cấu hình lại hệ thống thông tin, đảm bảo duy trì hoạt động của hệ thống thông tin; Kiểm soát quá trình cài đặt trên máy chủ.

e) Hệ thống mạng không dây (wireless) của các cơ quan, đơn vị phải được thiết lập các tham số: tên, nhận dạng dịch vụ (Service Set Identifier - SSID), thiết lập mật khẩu truy cập có độ phức tạp cao (độ dài tối thiểu 8 ký tự và bao gồm chữ hoa, chữ thường trong bảng chữ cái, số và các ký tự đặc biệt), mã hóa dữ liệu theo cơ chế bảo mật WPA2 hoặc WPA3.

g) 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.

h) 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; mật khẩu phải được đặt ở mức bảo mật, có độ phức tạp cao (độ dài tối thiểu 08 ký tự và bao gồm chữ hoa, chữ thường trong bảng chữ cái, số và các ký tự đặc biệt); mật khẩu phải thường xuyên thay đổi với tần suất tối thiểu 03 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.

i) Khuyến khích cài đặt, cấu hình, tổ chức hệ thống mạng nội bộ (LAN) theo mô hình Server-Client, hạn chế sử dụng mô hình mạng ngang hàng. Các cơ quan, đơn vị có nhiều phòng, ban, đơn vị trực thuộc không nằm trong cùng một khu vực, cần thiết lập mạng riêng ảo (VPN) để đảm bảo an toàn thông tin mạng cho mạng nội bộ.

k) Các cơ quan, đơn vị tham gia sử dụng mạng chuyên dùng thực hiện nghiêm túc các nội dung về bảo đảm an toàn thông tin mạng theo quy định về quản lý, vận hành, kết nối, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan Đảng, nhà nước.

5. Bảo đảm an toàn thông tin máy chủ

a) Thiết lập ghi lại nhật ký thông tin đăng nhập vào máy chủ, thông tin thay đổi cấu hình, thông tin truy cập dữ liệu và dịch vụ quan trọng trên máy chủ (nếu có).

b) Vô hiệu hóa, 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…

Điều 6. Bảo đảm an toàn thông tin máy tính

a) Tài khoản đăng nhập máy tính phải được thiết lập mật khẩu phức tạp; 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) Thay đổi các tài khoản mặc định trên máy tính hoặc vô hiệu hóa (nếu không sử dụng). Thiết lập giới hạn thời gian chờ (time out) để đóng các phiên truy cập, kết nối khi máy tính không nhận được yêu cầu từ người dùng.

c) Cài đặt phần mềm phòng, chống virút, mã độc có bản quyền cho tất cả các máy tính, đồng thời bảo đảm các phần mềm phòng, chống virút, mã độc này luôn được cập nhật, nhận dạng virút, mã độc mới; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm trên máy trạm khi chưa có sự đồng ý của người có thẩm quyền theo quy định của cơ quan.

d) Sử dụng các thiết bị lưu trữ (USB, ổ cứng di động) an toàn, đúng cách để phòng ngừa virút, 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 virút 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.

đ) 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 virút, phần mềm gián điệp được đính kèm theo thư và lây nhiễm vào máy tính.

e) Tất cả các máy tính của cơ quan, đơn vị phải được cấu hình nhằm vô hiệu hóa tính năng tự động thực thi các tập tin trên các thiết bị lưu trữ di động.

Điều 7. Bảo đảm an toàn thông tin đối với dữ liệu

a) Hệ thống thông tin của các cơ quan, đơn vị phải có cơ chế 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 sao lưu phải bảo đảm yêu cầu kỹ thuật; dữ liệu được sao lưu phải bảo đảm 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.

b) Trang bị hệ thống hoặc thiết bị lưu trữ dữ liệu (tủ hoặc băng, đĩa, DAS, NAS hoặc SAN) và tổ chức mô hình sao lưu độc lập (tách biệt về mặt vật lý) phù hợp với quy mô hệ thống thông tin của cơ quan, đơn vị.

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 nhật ký hoạt động cần thiết để phục vụ công tác điều tra, khắc phục khi xảy ra sự cố.

d) Thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

Điều 8. Bảo đảm an toàn thông tin cá nhân

1. Cán bộ, công chức, viên chức có trách nhiệm tự bảo vệ thông tin cá nhân của mình và tuân thủ các quy định tại khoản 1, khoản 2 Điều 10; khoản 1, khoản 4 Điều 16; khoản 3 Điều 17; khoản 1 Điều 18 Luật An toàn thông tin mạng và trong các văn bản pháp luật có liên quan.

Khi sử dụng, khai thác các hệ thống thông tin của cơ quan, đơn vị và các phần mềm ứng dụng dùng chung của tỉnh, có trách nhiệm:

a) Tự quản lý và chịu trách nhiệm về bảo vệ thông tin cá nhân đã được khai báo trong các hệ thống thông tin; không tiết lộ tài khoản đăng nhập, đấu nối, truy cập trái phép vào các phần mềm dùng chung của tỉnh.

b) Phải thực hiện việc đổi mật khẩu ngay sau khi được cấp tài khoản truy cập vào các phần mềm dùng chung của tỉnh, cơ quan, đơn vị.

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 quá trình sử dụng.

2. Các cơ quan, đơn vị, cá nhân khi xử lý thông tin cá nhân phải tuân thủ đầy đủ các nội dung theo quy định tại khoản 2, 3, 4, 5 Điều 16; khoản 1, 2 Điều 17; khoản 3 Điều 18; Điều 19 của Luật An toàn thông tin mạng và các quy định sau:

a) Quản lý và phân quyền truy cập trong các phần mềm ứng dụng, hệ thống thông tin, cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ, quyền hạn của người tham gia quản lý, vận hành, khai thác, sử dụng các phần mềm ứng dụng, hệ thống thông tin, cơ sở dữ liệu.

b) Khi cán bộ, công chức, viên chức đã nghỉ việc hoặc chuyển công tác, các cơ quan, đơn vị phải thực hiện việc thu hồi các thiết bị công nghệ thông tin liên quan; đồng thời phải thông báo ngay bằng văn bản đến cơ quan quản lý, quản trị phần mềm ứng dụng, hệ thống thông tin, cơ sở dữ liệu để thực hiện các biện pháp kỹ thuật cập nhật lại, khóa hoặc hủy tài khoản người dùng.

3. Sở Thông tin và Truyền thông thực hiện công tác quản lý nhà nước về bảo vệ thông tin cá nhân trên mạng theo các nội dung quy định tại Điều 20 của Luật An toàn thông tin mạng.

Điều 9. Giám sát an toàn thông tin mạng cho các hệ thống thông tin

1. Tổ chức thực hiện việc giám sát an toàn hệ thống thông tin của cơ quan, đơn vị trực tiếp quản lý. Nội dung và đối tượng giám sát thực hiện theo quy định tại các khoản 1, khoản 2 Điều 24 của Luật An toàn thông tin mạng; thực hiện việc lưu trữ nhật ký tình trạng hoạt động của các hệ thống thông tin tại các máy chủ trong thời gian ít nhất là 30 ngày để phục vụ các công tác đảm bảo an toàn thông tin mạng.

2. Bảo đảm duy trì việc kết nối, chia sẻ dữ liệu giám sát theo thời gian thực của các hệ thống thông tin về Trung tâm Giám sát an toàn không gian mạng quốc gia. Thiết lập chế độ chia sẻ dữ liệu giám sát phù hợp để bảo đảm chất lượng chia sẻ.

Điều 10. Bảo vệ bí mật Nhà nước trong công tác ứng dụng công nghệ thông tin, chuyển đổi số

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 được in, sao chụp tài liệu bí mật nhà nước trên các thiết bị kết nối mạng; Không bật các thiết bị kết nối mạng trong các cuộc họp có nội dung bí mật nhà nước.

3. 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, công chức có thẩm quyền.

4. 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.

5. 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 11. Công chức, viên chức được phân công thực hiện nhiệm vụ hoặc chuyên trách về công nghệ thông tin

1. Được bảo đảm 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 thông tin mạng, 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 bảo đảm an toàn thông tin mạng trong toàn hệ thống; triển khai các giải pháp kỹ thuật chống virút, 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 virút.

6. Cấu hình hệ thống với những chính sách bảo mật phù hợp hoạt động của hệ thống thông tin của 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 ngăn cấm hoặc hạn chế.

7. Thường xuyên sao lưu dữ liệu theo quy định; kiểm tra dữ liệu sao lưu phải bảo đảm 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. Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm tra, phát hiện, phòng ngừa, đấu tranh, ngăn chặn xâm phạm an toàn thông tin; tham gia khắc phục sự cố về an toàn thông tin mạng.

10. Thường xuyên thực hiện phân tích, đánh giá và báo cáo các rủi ro và nguy cơ mất an toàn thông tin mạng đối với hệ thống thông tin của cơ quan, đơn vị; nguyên nhân gây ra các rủi ro và nguy cơ mất an toàn thông tin bao gồm: hiện tượng tự nhiên (nhiệt độ, không khí, mưa bão, sét,…), truy cập trái phép, virút, 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 12. Giải quyết và khắc phục sự cố về an toàn thông tin mạng

1. Đối với người sử dụng

a) Thông tin, báo cáo kịp thời cho công chức, viên chức thực hiện nhiệm vụ hoặc chuyên trách về công nghệ thông tin của cơ quan, đơn vị khi phát hiện các sự cố gây mất an toàn thông tin, an ninh mạng 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 công chức, viên chức thực hiện nhiệm vụ hoặc chuyên trách về công nghệ thông tin

a) Xử lý khẩn cấp: Khi phát hiện hệ thống có nguy cơ mất an toàn thông tin như hệ thống hoạt động chậm bất thường, không truy cập được hệ thống ứng dụng, nội dung cổng (trang) thông tin điện tử hoặc giao diện ứng dụng bị thay đổi, các sự cố khác có liên quan thực hiện các bước cơ bản như sau:

Bước 1: Ngắt kết nối hệ thống máy chủ ra khỏi hệ thống mạng, báo cáo sự cố đến Thủ trưởng cơ quan, đơn vị;

Bước 2: Sao chép nhật ký truy cập của người dùng (logfile) và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ (phục vụ cho công tác phân tích);

Bước 3: Khôi phục lại hệ thống, hoặc sử dụng hệ thống dự phòng và chuyển dữ liệu sao lưu dự phòng (backup) mới nhất để hệ thống hoạt động trở lại bình thường;

Lập biên bản ghi nhận sự cố gây mất an toàn 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.

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

3. Sở Thông tin và Truyền thông

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 thông tin mạng.

b) Chỉ đạo các đơn vị trực thuộc nhanh chóng hỗ trợ, phối hợp và hướng dẫn các cơ quan, đơn vị khắc phục sự cố về an toàn thông tin mạng.

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 thông tin mạng.

d) Phối hợp với Công an tỉnh trong điều tra làm rõ các nguyên nhân gây ra sự cố về an ninh, an toàn thông tin mạng.

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

Chương III
TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 13. 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 bảo đảm an toàn thông tin, an ninh mạng đối với toàn bộ hệ thống thông tin của cơ quan, đơn vị thuộc thẩm quyền quản lý.

2. Xây dựng, triển khai kế hoạch bảo đảm an toàn thông tin mạng và báo cáo định kỳ hàng năm (ngày 25 tháng 10) hoặc đột xuất theo yêu cầu về Sở Thông tin và Truyền thông để tổng hợp, báo cáo Ủy ban nhân dân tỉnh, Bộ Thông tin và Truyền thông; hàng năm cân đối, bố trí kinh phí bảo đảm an toàn thông tin mạng trong nội bộ cơ quan, đơn vị; đầu tư các thiết bị phần cứng, phần mềm liên quan đến công tác bảo đảm an toàn thông tin mạng.

3. Tuân thủ và bảo đảm an toàn thông tin trong ứng dụng công nghệ thông tin, chuyển đổi số, đảm bảo an toàn thông tin mạng nội bộ của cơ quan, đơn vị theo quy định của Quy chế này và các quy định khác của pháp luật có liên quan.

4. Tuyên truyền, phổ biến Quy chế này và các quy định khác của pháp luật có liên quan về an toàn thông tin mạng, an ninh mạng trong phạm vi trách nhiệm và quyền hạn của từng cơ quan, đơn vị.

5. Thực hiện xác định và trình cấp có thẩm quyền phê duyệt cấp độ an toàn hệ thống thông tin và bảo đảm an toàn thông tin mạng cho hệ thống thông tin của cơ quan, đơn vị theo quy định tại Luật An toàn thông tin mạng, Nghị định số 85/2016/NĐ-CP và hướng dẫn tại Thông tư số 12/2022/TT-BTTTT.

6. Phối hợp với Sở Thông tin và Truyền thông trong công tác giám sát an toàn thông tin mạng đối với các hệ thống thông tin của cơ quan, đơn vị.

7. Khi có sự cố hoặc nguy cơ mất an toàn 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, đồng thời lập biên bản và báo cáo bằng văn bản cho cơ quan liên quan.

8. Tạo điều kiện thuận lợi cho các cơ quan chức năng trong công tác điều tra, làm rõ nguyên nhân gây ra sự cố; lực lượng kỹ thuật tham gia khắc phục sự cố thực hiện đúng theo hướng dẫn chuyên môn của Sở Thông tin và Truyền thông.

9. Phối hợp chặt chẽ với Sở Thông tin và Truyền thông, Công an tỉnh 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 mạng.

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

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

2. Thực hiện công tác tham mưu Ủy ban nhân dân tỉnh ban hành:

a) Văn bản chỉ đạo, kế hoạch, đề án nhằm bảo đảm an toàn thông tin mạng.

b) Thực hiện thủ tục xác định cấp độ an toàn thông tin mạng và bảo đảm an toàn cho các hệ thống thông tin theo quy định của Luật An toàn thông tin mạng, Nghị định số 85/2016/NĐ-CP và hướng dẫn tại Thông tư số 12/2022/TT-BTTTT.

c) Chủ trì thành lập đoàn kiểm tra về bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số trong các cơ quan nhà nước khi cần thiết.

3. Quản lý vận hành, hướng dẫn kết nối mạng truyền số liệu chuyên dùng của các cơ quan Đảng, nhà nước trên địa bàn tỉnh; xử lý các vấn đề liên quan sự cố mạng truyền số liệu chuyên dùng.

4. Tổ chức đào tạo chuyên sâu về an toàn thông tin mạng cho lực lượng bảo đảm an toàn thông tin mạng của các cơ quan, đơn vị.

5. Tổ chức Hội nghị, Hội thảo chuyên đề về an toàn thông tin mạng; phối hợp với Công an tỉnh tổ chức Hội nghị, Hội thảo chuyên đề về an ninh mạng.

6. Phối hợp với Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC) và các đơn vị có liên quan trong thực hiện nhiệm vụ bảo đảm an toàn thông tin mạng; cảnh báo các vấn đề về an toàn thông tin trong các cơ quan nhà nước trên địa bàn tỉnh.

7. Phối hợp với Công an tỉnh và các cơ quan, đơn vị có liên quan tổ chức đoàn kiểm tra về an toàn thông tin, an ninh mạng để kịp thời phát hiện, xử lý các hành vi vi phạm theo thẩm quyền.

8. Đề nghị Ủy ban nhân dân tỉnh khen thưởng hoặc phê bình Thủ trưởng cơ quan, đơn vị trong thực hiện chỉ đạo về bảo đảm an toàn thông tin mạng.

9. Tổng hợp, báo cáo và thông báo về tình hình an toàn thông tin mạng theo định kỳ cho Ủy ban nhân dân tỉnh, Bộ Thông tin và Truyền thông.

10. Chỉ đạo Trung tâm Công nghệ thông tin và Truyền thông triển khai thực hiện công tác giám sát an toàn thông tin mạng đối với các hệ thống thông tin đang cài đặt, vận hành tại Trung tâm Tích hợp Dữ liệu tỉnh, các hệ thống thông tin của các cơ quan, đơn vị có kết nối đến Trung tâm Tích hợp Dữ liệu tỉnh theo quy định; kịp thời cung cấp các thông tin, dữ liệu có liên quan cho các cơ quan chức năng có thẩm quyền để phục vụ công tác điều tra, xác minh an toàn thông tin mạng khi có yêu cầu.

11. Phối hợp với Ban Cơ yếu Chính phủ tổ chức triển khai ứng dụng chữ ký số cho các cơ quan, đơn vị trên địa bàn tỉnh nhằm bảo đảm an toàn thông tin mạng trong các giao dịch điện tử.

12. Tham gia mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia và thực hiện trách nhiệm, quyền hạn của thành viên mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia theo quy định tại Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.

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 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 thông tin và trật tự an toàn xã hội trên địa bàn tỉnh.

2. Phối hợp với các cơ quan chức năng trong trao đổi, kiểm tra, bảo đảm an ninh, an toàn thông tin mạng.

3. 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 ninh, an toàn thông tin mạng.

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

5. 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.

6. Hàng năm, chủ trì tổ chức tập huấn về công tác an toàn, an ninh thông tin trên môi trường mạng cho các cơ quan, đơn vị.

Điều 16. Trách nhiệm của Tổ Ứng cứu sự cố an toàn thông tin mạng

1. Triển khai các giải pháp nhằm hỗ trợ các cơ quan, đơn vị trên địa bàn tỉnh về công tác bảo đảm an toàn thông tin mạng, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số.

2. Phối hợp kiểm tra an toàn thông tin, an ninh mạng đối với hệ thống thông tin của các cơ quan, đơn vị.

3. Tổ chức diễn tập ứng cứu sự cố mất an toàn thông tin mạng.

4. Điều phối các hoạt động ứng cứu sự cố về an toàn thông tin mạng và tổ chức ứng cứu sự cố an toàn thông tin mạng tại các cơ quan, đơn vị trên địa bàn tỉnh.

Điều 17. Trách nhiệm của cá nhân tham gia sử dụng và khai thác hệ thống thông tin tại các cơ quan, đơn vị

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

2. Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo kịp thời cho công chức, viên chức thực hiện nhiệm vụ hoặc chuyên trách về công nghệ thông tin của cơ quan, đơn vị mình để kịp thời ngăn chặn và xử lý.

3. Nâng cao ý thức cảnh giác và trách nhiệm về an toàn thông tin, an ninh mạng.

4. Các thông tin, tài liệu, văn bản có tính mật theo quy định, phải dự thảo, lưu trữ đúng theo quy định về bảo mật và an toàn thông tin.

5. Không được truy cập vào các liên kết (link) không rõ ràng; không sử dụng địa chỉ thư điện tử công vụ vào mục đích cá nhân như: đăng ký tài khoản mạng xã hội, đăng ký mua sắm qua mạng; Không sử dụng mạng xã hội như: Google Plus+, MySpace, LinkedIn, Twitter, Facebook, Zalo, blog cá nhân để đăng tải, phát tán, truyền tải lại những nội dung phản động, tuyên truyền, xuyên tạc.

Điều 18. Trách nhiệm của tổ chức, doanh nghiệp, cá nhân có liên quan đối với việc bảo đảm an toàn thông tin mạng

1. Các tổ chức, doanh nghiệp cung cấp dịch vụ hạ tầng mạng, Internet, công nghệ thông tin 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 đối với các 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 thông tin mạng, an ninh mạng 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 thông tin trên mạng.

3. Các tổ chức, cá nhân khác có sử dụng các hệ thống thông tin do Ủy ban nhân dân tỉnh triển khai hoặc liên quan đến hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước phải tuân thủ Quy chế này và các quy định hiện hành của pháp luật có liên quan.

Điều 19. Trách nhiệm của Sở Tài chính

Phối hợp với Sở Thông tin và truyền thông đảm bảo kinh phí thực hiện các nội dung về đảm bảo an toàn, an ninh thông tin trên môi trường mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh từ nguồn chi thường xuyên hàng năm theo quy định.

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

Điều 20. Kiểm tra định kỳ và đột xuất

1. Sở Thông tin và Truyền thông chủ trì, phối hợp với đoàn kiểm tra xây dựng kế hoạch và thực hiện kiểm tra định kỳ về công tác bảo đảm an toàn thông tin mạng, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của các cơ quan nhà nước.

2. Sở Thông tin và Truyền thông phối hợp với Công an tỉnh và các đơn vị có liên quan tiến hành kiểm tra đột xuất các cơ quan, đơn vị có dấu hiệu vi phạm về an toàn thông tin mạng, an ninh mạng.

Điều 21. 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 và công chức, viên chức thực hiện nhiệm vụ hoặc chuyên trách về 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 22. Tổ chức thực hiện

1. Sở Thông tin và Truyền thông chủ trì, phối hợp với các cơ quan, đơn vị, địa phương triển khai thực hiện Quy chế này.

2. Thủ trưởng các cơ quan, đơn vị, địa phương tổ chức triển khai thực hiện nghiêm túc Quy chế này.

3. Các văn bản quy phạm pháp luật dẫn chiếu để áp dụng tại Quy chế này được sửa đổi, bổ sung hoặc thay thế bằng văn bản mới thì áp dụng theo các văn bản sửa đổi, bổ sung hoặc thay thế.

4. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, phát sinh cần sửa đổi, bổ sung, đề nghị các cơ quan, đơn vị kịp thời báo cáo về Sở Thông tin và Truyền thông để tổng hợp trình Ủy ban nhân dân tỉnh xem xét, quyết định./.