ỦY BAN NHÂN DÂN TỈNH LONG AN
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

QUY ĐỊNH VỀ ĐẢM BẢO AN TOÀN THÔNG TIN TRONG HOẠT ĐỘNG ỨNG DỤNG CNTT CỦA CƠ QUAN NHÀ NƯỚC TRÊN ĐỊA BÀN TỈNH LONG AN

(Quyết định số 49/2014/QĐ-UBND ngày 03/10/2014 của UBND tỉnh)

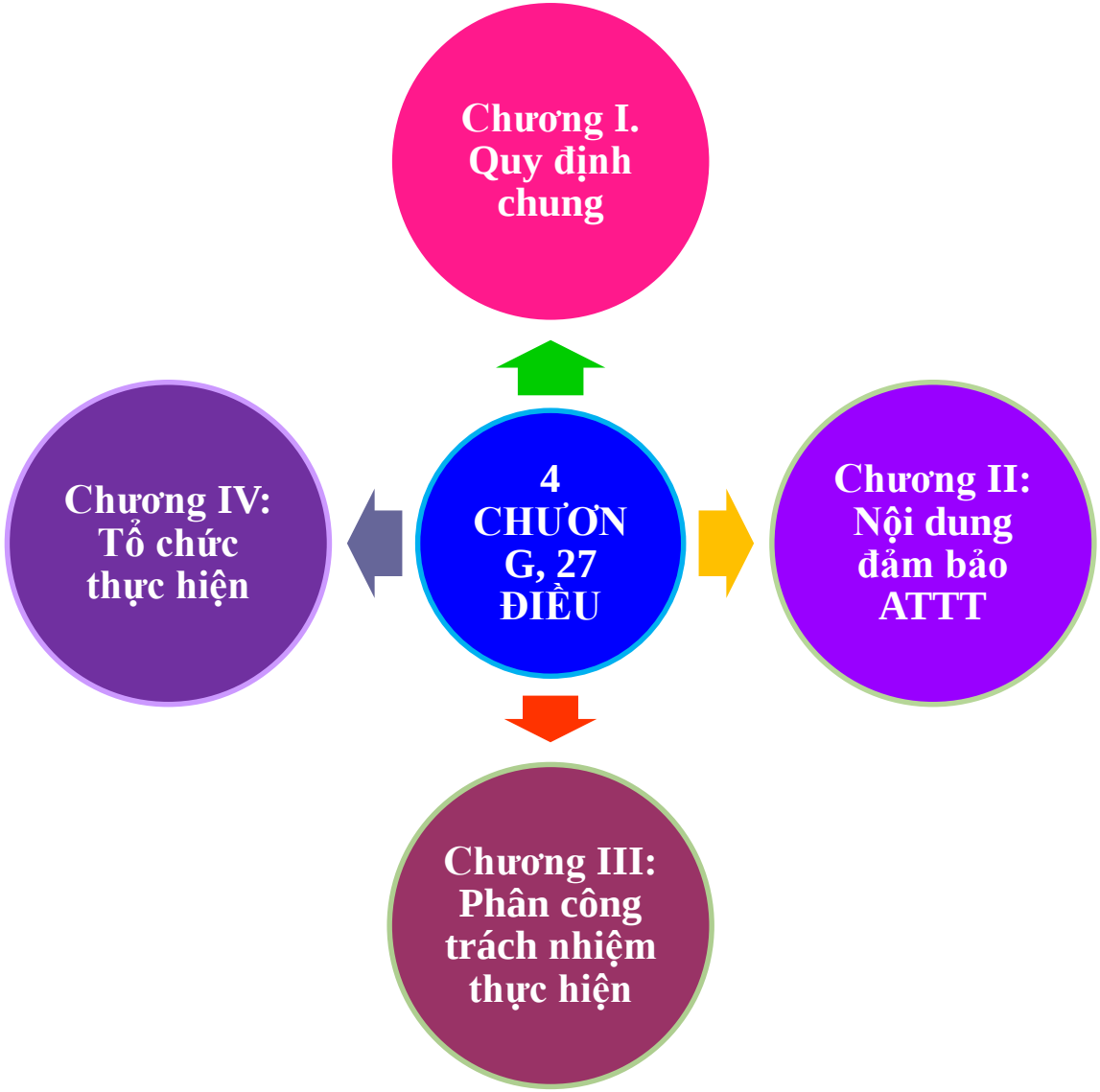
Người trình bày: Tăng Thị Ngọc Em – TP. CNTT Sở TTTT

Ngày 25 tháng 11 năm 2016

QUYẾT ĐỊNH SỐ 49/2014/QĐ-UBND

- Có hiệu lực thi hành từ ngày 13/10/2014
- Thay thế Quyết định số 49/2010/QĐ-UBND ngày 01/12/2010 của UBND tỉnh về việc ban hành quy định về đảm bảo an toàn, an ninh thông tin và bảo mật trên môi trường mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Long An

BỐ CỤC


Chương I. Quy định chung
Chương IV: Tổ chức thực hiện
4 CHƯƠNG, 27 ĐIỀU
Chương II: Nội dung đảm bảo ATTT
Chương III: Phân công trách nhiệm thực hiện

NỘI DUNG

1. Quy định chung
2. Đảm bảo ATTT đối với cơ sở hạ tầng
3. Đảm bảo ATTT đối với phần mềm ứng dụng
4. Tổ chức thực hiện

1. QUY ĐỊNH CHUNG

I. Phạm vi và đối tượng áp dụng

1

- Quy định về công tác đảm bảo ATTT số và trách nhiệm của tổ chức, cá nhân có liên quan trong hoạt động ứng dụng CNTT trên môi trường mạng của các CQNN trên địa bàn tỉnh.

2

- Áp dụng cho UBND các cấp, sở ngành tỉnh; các đơn vị sự nghiệp trên địa bàn tỉnh; các tổ chức đoàn thể tỉnh; các cơ quan chuyên môn, đơn vị thuộc UBND cấp huyện.

3

- CBCC-VC, người lao động trong các cơ quan, đơn vị nêu tại mục 1 và các tổ chức, cá nhân có liên quan đến hoạt động ứng dụng CNTT trên môi trường mạng của các CQNN.

II. Nguyên tắc chung đảm bảo ATTT

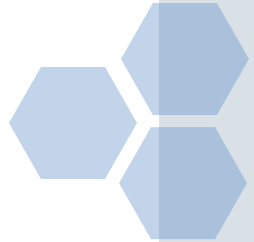
- Không được xâm phạm ATTT.
- Phát hiện hành vi xâm phạm ATTT hoặc sự cố mất ATTT có trách nhiệm thông báo kịp thời cho cơ quan chức năng liên quan.
- Có trách nhiệm bảo đảm ATTT đối với thông tin và hệ thống thông tin thuộc thẩm quyền quản lý.
- Tuân thủ các nguyên tắc, các tiêu chuẩn, quy chuẩn kỹ thuật về bảo mật, ATTT số.

II. Nguyên tắc chung đảm bảo ATTT

- Triển khai các giải pháp tăng cường khả năng phòng, chống các nguy cơ tấn công, xâm nhập các hệ thống thông tin.

- Ngăn chặn, khắc phục kịp thời các sự cố mất ATTT trên mạng máy tính và các hệ thống thông tin thuộc thẩm quyền quản lý.

- Ngăn ngừa việc lộ, lọt tài liệu, thông tin bí mật nhà nước.



III. Hành vi bị nghiêm cấm

- Tuyên truyền chống lại Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam.

- Tiết lộ bí mật nhà nước và những bí mật khác do pháp luật quy định.

- Đưa thông tin xuyên tạc, vu khống, xúc phạm uy tín của tổ chức, danh dự và nhân phẩm của cá nhân.

- Ngăn chặn trái phép việc truyền tải thông tin trên mạng; can thiệp trái phép, gây nguy hại, xóa, thay đổi, sửa chữa làm sai lệch thông tin trên mạng.

III. Hành vi bị nghiêm cấm

- Đánh cắp và sử dụng trái phép mật khẩu, khoá mật mã, thông tin riêng của tổ chức, cá nhân; ngăn cản bất hợp pháp việc truy nhập thông tin của tổ chức, cá nhân.

- Cản trở bất hợp pháp, gây ảnh hưởng tới hoạt động bình thường của hệ thống thông tin; Lợi dụng sơ hở, điểm yếu của hệ thống thông tin để vô hiệu hóa, vượt qua biện pháp kiểm soát truy cập, tấn công, chiếm quyền điều khiển trái phép đối với hệ thống thông tin.

- Phát tán thư rác, thư giả mạo, tin nhắn rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.

2. ĐẢM BẢO AN TOÀN THÔNG TIN ĐỐI VỚI CƠ SỞ HẠ TẦNG

I. Đảm bảo an toàn sử dụng máy tính làm việc

- Máy tính làm việc chỉ được cài đặt phần mềm thông dụng.
- Hệ điều hành được cập nhật bản vá lỗi kịp thời, cài đặt phần mềm phòng chống, diệt virus có bản quyền.
- Thường xuyên rà quét để phát hiện và loại bỏ mã độc trong máy tính.
- Không tự ý thay đổi cấu hình máy tính, kết nối máy tính cá nhân do cơ quan cấp vào các mạng thông tin khác (ngoài hệ thống thông tin của cơ quan).

I. Đảm bảo an toàn sử dụng máy tính làm việc

- Không tự ý sử dụng máy tính được cấp cho người sử dụng khác.
- Phải sử dụng mật khẩu mạnh cho tài khoản đăng nhập vào máy tính.
- Khi sử dụng các thiết bị lưu trữ di động cá nhân phải tiến hành quét virus trước khi đưa vào sử dụng trên máy tính làm việc của mình.
- Không được kết nối điện thoại thông minh, máy tính bảng với hệ thống nội bộ khi chưa có sự cho phép của lãnh đạo cơ quan, đơn vị.

II. Đảm bảo ATTT khi kết nối và sử dụng mạng Internet

- Không được phép truy cập các trang thông tin có nghi ngờ chứa mã độc, không rõ nguồn gốc hoặc có nội dung không phù hợp (*phản động hoặc trái thuần phong mỹ tục*). Ngoại trừ những người có chức năng, thẩm quyền QLNN lĩnh vực Internet có quyền truy cập để phục vụ cho công tác điều tra, xử lý.

- Nghiêm cấm dùng máy tính kết nối vào hệ thống mạng để soạn thảo, in ấn, sao chép, lưu trữ tài liệu có nội dung liên quan đến bí mật Nhà nước.

III. Đảm bảo an toàn trong thu hồi, thanh lý, sửa chữa thiết bị

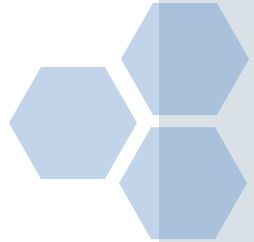
- Các thiết bị (máy chủ, máy tính xách tay, phương tiện lưu trữ, máy tính để bàn, smartphone,…) khi không còn sử dụng cho công việc của cơ quan, đơn vị thì tiến hành thu hồi, thanh lý và đơn vị đang sử dụng, quản lý phải tiến hành xóa dữ liệu, ghi đè hoặc phá hủy vật lý, đảm bảo dữ liệu được xoá không thể khôi phục lại được.

- Đối với các phương tiện lưu trữ có chứa dữ liệu quan trọng, phương án xử lý và ghi đè dữ liệu phải được bộ phận chuyên trách CNTT xem xét và có ý kiến phê duyệt của lãnh đạo cơ quan, đơn vị.

III. Đảm bảo an toàn trong thu hồi, thanh lý, sửa chữa thiết bị

- Trường hợp bắt buộc phải sửa chữa, bảo hành các thiết bị (*máy chủ, máy tính để bàn, máy tính xách tay, ổ cứng, thiết bị lưu trữ di động,...*) phải có ý kiến của bộ phận chuyên trách CNTT và được lãnh đạo phê duyệt.

- Trường hợp bàn giao các thiết bị (*máy chủ, máy tính để bàn, máy tính xách tay, các thiết bị lưu trữ, ...*) cho bên thứ ba sửa chữa phải có biện pháp đảm bảo dữ liệu bên trong thiết bị được an toàn, không bị lộ, lọt thông tin, dữ liệu.



3. ĐẢM BẢO AN TOÀN THÔNG TIN ĐỐI VỚI PHẦN MỀM ỨNG DỤNG

I. Đảm bảo an toàn cơ sở dữ liệu

- Áp dụng chữ ký số để xác thực và bảo mật dữ liệu.
- Văn bản điện tử có nội dung cần hạn chế tiếp cận nhưng không thuộc danh mục bí mật Nhà nước được sử dụng tính năng mã hoá (đặt mật khẩu) của các ứng dụng văn phòng (phần mềm soạn thảo, đọc văn bản, nén tập tin), nhưng phải sử dụng mật khẩu an toàn.
- CBCC-VC thực hiện soạn thảo, gửi, nhận dữ liệu có trách nhiệm xác định mức độ quan trọng của dữ liệu để thực hiện phương thức bảo vệ dữ liệu phù hợp hoặc yêu cầu bộ phận chuyên trách CNTT hướng dẫn, hỗ trợ phương thức bảo vệ trong trường hợp cần thiết.

I. Đảm bảo an toàn cơ sở dữ liệu

- Cơ quan, đơn vị, CBCC-VC, người lao động bắt buộc phải sử dụng hộp thư điện tử của tỉnh *(@longan.gov.vn)* hoặc của ngành dọc *(.gov.vn)* để trao đổi thông tin, gửi nhận tài liệu, văn bản phục vụ cho công việc. Tuyệt đối không được sử dụng các địa chỉ thư điện tử miễn phí khác (gmail, yahoo mail,...) để trao đổi thông tin, gửi nhận tài liệu phục vụ cho công việc.

II. Quản lý, sử dụng tài khoản và mật khẩu

- Mật khẩu của tất cả các tài khoản (ở cả cấp độ quản trị hệ thống và cấp độ người sử dụng) phải tuân thủ đồng thời các yêu cầu sau:
  - Có chứa cả các ký tự chữ in và chữ thường
  - Có chứa ký tự số, các ký tự dấu câu hoặc các ký tự đặc biệt (!, @, #, ...)
  - Có ít nhất 08 ký tự đối với tài khoản người dùng, ít nhất 15 ký tự đối với tài khoản quản trị hệ thống
  - Không phải là một dãy ký tự lặp lại có quy luật
  - Không dựa vào thông tin cá nhân (ngày sinh, số điện thoại,…), tên người, tên địa danh, tên cơ quan hoặc các tên gọi khác

II. Quản lý, sử dụng tài khoản và mật khẩu

- Người dùng phải thay đổi mật khẩu ngay lần đầu tiên đăng nhập vào hệ thống và thường xuyên thay đổi mật khẩu ít nhất 03 tháng/01 lần.

- Khi quên mật khẩu hoặc nghi ngờ mật khẩu tài khoản của mình bị người khác biết ngoài ý muốn, phải báo cáo sự việc với thủ trưởng cơ quan và cán bộ chuyên trách CNTT để có phương án xử lý kịp thời.

- Không sử dụng mật khẩu đã bị đánh cắp hoặc nghi ngờ bị đánh cắp cho tài khoản cũ hoặc các tài khoản khác do cơ quan cấp.

4. TỔ CHỨC THỰC HIỆN

I. Phân công trách nhiệm thực hiện

1. Trách nhiệm của các cơ quan, đơn vị
2. Trách nhiệm Sở Thông tin và Truyền thông
3. Trách nhiệm Công an tỉnh
4. Trách nhiệm Sở Tài chính
5. Trách nhiệm Sở Kế hoạch và Đầu tư
6. Trách nhiệm của cán bộ, công chức, viên chức, người lao động

II. Trách nhiệm của CBCCVC-LĐ

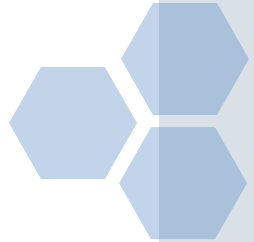
- Cán bộ chuyên trách CNTT có trách nhiệm tham mưu thủ trưởng cơ quan, đơn vị:
  - Triển khai thực hiện các biện pháp quản lý vận hành kỹ thuật cho hệ thống thông tin của cơ quan, đơn vị mình.
  - Phối hợp với các cơ quan, đơn vị, cá nhân có liên quan trong việc kiểm tra, phát hiện và khắc phục các sự cố mất ATTT.
  - Tham gia các chương trình đào tạo, hội nghị về ATTT do tỉnh hoặc các đơn vị chuyên môn tổ chức.
  - Xác định các chương trình, phần mềm cần thiết để cài đặt trên các máy tính cá nhân trong cơ quan phục vụ công việc của từng nhóm người dùng (văn thư, cán bộ chuyên môn, kế toán, ...).

II. Trách nhiệm của CBCCVC-LĐ

- CBCC-VC, người lao động có trách nhiệm:

  - Chấp hành nghiêm các quy định của tỉnh, cơ quan, đơn vị về công tác đảm bảo ATTT và các quy định pháp luật khác có liên quan; nâng cao ý thức cảnh giác và có trách nhiệm trong công tác đảm bảo ATTT tại cơ quan, đơn vị.

  - Khi phát hiện sự cố mất ATTT phải báo cáo ngay với lãnh đạo trực tiếp và bộ phận hoặc cán bộ chuyên trách CNTT để kịp thời ngăn chặn, xử lý.



III. Trách nhiệm Sở Thông tin và Truyền thông

Xin cảm ơn!