UBND TỈNH AN GIANG
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 28/QĐ-STTTT

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

An Giang, ngày 14 tháng 3 năm 2024

QUYẾT ĐỊNH

Về việc ban hành Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống thông tin của Trung tâm Tích hợp dữ liệu tỉnh An Giang

GIÁM ĐỐC SỞ THÔNG TIN VÀ TRUYỀN THÔNG TỈNH AN GIANG

Căn cứ Luật Công nghệ thông tin năm 2006 (sửa đổi, bổ sung năm 2017);

Căn cứ Luật An toàn thông tin mạng năm 2015;

Căn cứ Luật An ninh mạng năm 2018;

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

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông về việc quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP;

Căn cứ Quyết định số 47/2022/QĐ-UBND ngày 12/12/2022 của Ủy ban nhân dân tỉnh An Giang về việc Ban hành Quy định về chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Thông tin và Truyền thông tỉnh An Giang;

Căn cứ Quyết định số 396/QĐ-UBND ngày 07 tháng 3 năm 2022 của Chủ tịch Ủy ban nhân dân tỉnh An Giang về việc thành lập Trung tâm Công nghệ thông tin và Truyền thông trên cơ sở hợp nhất Trung tâm Tin học và Trung tâm Dịch vụ Công nghệ thông tin và Truyền thông;

Theo đề nghị của Giám đốc Trung tâm Công nghệ thông tin và Truyền thông,

QUYẾT ĐỊNH:

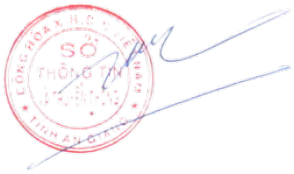
Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn, an ninh thông tin mạng của Hệ thống thông tin tại Trung tâm Tích hợp dữ liệu tỉnh An Giang.

Điều 2. Quyết định này có hiệu lực từ ngày ký.

Điều 3. Ban Giám đốc, Lãnh đạo các phòng, Trung tâm và toàn thể công chức, viên chức, người lao động Sở Thông tin và Truyền thông; các cơ quan, tổ chức, cá nhân có kết nối, sử dụng hệ thống thông tin Trung tâm Tích hợp dữ liệu tỉnh và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Sở TTTT: BGĐ, các phòng và Trung tâm;
- Lưu: VT, TTCNTTTT.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC



Nguyễn Thanh Hải

UBND TỈNH AN GIANG
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

QUY CHẾ
Bảo đảm an toàn, an ninh mạng Hệ thống thông tin tại Trung tâm Tích hợp dữ liệu tỉnh An Giang

(Ban hành kèm theo Quyết định số: 28/QĐ-STTTT ngày 14 tháng 3 năm 2024)

Chương I:
QUY ĐỊNH CHUNG

Điều 1. Phạm vi và đối tượng áp dụng

1. Phạm vi

Quy chế này quy định các chính sách quản lý và các biện pháp nhằm bảo đảm an toàn thông tin (ATTT) cho Hệ thống thông tin Trung tâm Tích hợp dữ liệu tỉnh An Giang (TTTHDL) bao gồm:

a) Phạm vi quản lý về vật lý và logic của Hệ thống;

b) Các ứng dụng, dịch vụ hệ thống cung cấp;

c) Nguồn nhân lực bảo đảm ATTT.

2. Đối tượng áp dụng

a) Các đơn vị thuộc Sở Thông tin và Truyền thông; công chức, viên chức và người lao động thuộc Sở Thông tin và Truyền thông.

b) Cơ quan, tổ chức, cá nhân có kết nối, sử dụng Hệ thống thông tin TTTHDL tỉnh.

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ quản lý, vận hành, duy trì, phát triển và bảo đảm ATTT mạng, phục vụ hoạt động của Hệ thống thông tin TTTHDL tỉnh.

Điều 2. Giải thích từ ngữ

Trong quy chế này, các từ ngữ dưới đây được hiểu như sau:

1. *An toàn thông tin mạng* là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

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

3. *Hệ thống thông tin* là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng.

4. *Chủ quản hệ thống thông tin* là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin.

5. *Sự cố an toàn thông tin mạng* là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

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. *Thông tin cá nhân* là thông tin gắn với việc xác định danh tính của một người cụ thể.

8. *Xử lý thông tin cá nhân* là việc thực hiện một hoặc một số thao tác thu thập, biên tập, sử dụng, lưu trữ, cung cấp, chia sẻ, phát tán thông tin cá nhân trên mạng nhằm mục đích thương mại.

9. *Không gian mạng* là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin (CNTT), bao gồm mạng viễn thông, mạng internet, hệ thống máy tính, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian.

10. Các thuật ngữ, tên công nghệ phổ biến được nêu trong Quy chế này:

SSL (Secure Sockets Layer): Giao thức mã hóa kênh truyền dữ liệu kết nối an toàn giữa máy chủ web (host) và trình duyệt web (client) web.

TLS (Transport Layer Security): Giao thức Bảo mật tầng vận chuyển, giao thức mật mã cung cấp bảo mật đầu cuối cho dữ liệu được gửi giữa các ứng dụng qua Internet.

SSH (Secure Shell): đây là một giao thức hỗ trợ các nhà quản trị mạng truy cập vào máy chủ từ xa thông qua mạng internet không bảo mật.

VPN (Virtual Private Network): mạng riêng ảo, là một công nghệ mạng giúp tạo kết nối mạng an toàn khi tham gia vào mạng công cộng như Internet hoặc mạng riêng do một nhà cung cấp dịch vụ sở hữu, để cho phép người dùng từ xa kết nối an toàn đến mạng riêng của cơ quan mình.

LAN (Local Area Network): mạng cục bộ, mạng nội bộ kết nối máy tính, thiết bị tại mỗi phòng ban, cơ quan, đơn vị, có thể sử dụng kết nối giao thức TCP/IP (Transmission Control Protocol/Internet Protocol: giao thức điều khiển truyền nhận/ Giao thức liên mạng, một bộ các giao thức truyền thông được sử dụng để kết nối các thiết bị mạng với nhau trên internet. TCP/IP cũng có thể được sử dụng như một giao thức truyền thông trong mạng máy tính riêng (mạng nội bộ) có dây hoặc không dây).

Điều 3. Mục tiêu, nguyên tắc bảo đảm ATTT

1. Mục tiêu bảo đảm ATTT

Bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn,

tính bảo mật và tính khả dụng của Hệ thống thông tin TTTHDL tỉnh.

2. Nguyên tắc

a) Cơ quan, tổ chức thuộc đối tượng áp dụng Quy chế này có trách nhiệm bảo đảm ATTT và hệ thống thông tin trong phạm vi xử lý công việc của mình theo quy định của pháp luật, hướng dẫn của cơ quan, đơn vị có thẩm quyền và các quy định tại Quy chế này.

b) Bảo đảm ATTT là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục trong quá trình:

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

- Thiết kế, thiết lập và vận hành, nâng cấp, hủy bỏ hệ thống thông tin.

c) Việc bảo đảm an toàn Hệ thống thông tin TTTHDL tỉnh được thực hiện một cách tổng thể, đồng bộ, tập trung trong việc đầu tư các giải pháp bảo vệ, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp.

d) Các đơn vị trực thuộc Sở có trách nhiệm bảo đảm an toàn, an ninh thông tin mạng của đơn vị mình; bố trí nhân sự chịu trách nhiệm bảo đảm an toàn, an ninh thông tin mạng; xác định rõ quyền hạn, trách nhiệm của Thủ trưởng đơn vị, từng bộ phận, cá nhân trong đơn vị đối với công tác bảo đảm an toàn, an ninh thông tin mạng.

Điều 4. Những hành vi nghiêm cấm

1. Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật An ninh mạng và Điều 8 Luật An ninh mạng.

2. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập mạng không dây của cá nhân vào mạng nội bộ.

3. Tự ý thay đổi, gỡ bỏ biện pháp ATTT cài đặt trên thiết bị CNTT phục vụ công việc; tự ý thay thế, lắp mới, tráo đổi thành phần của máy tính phục vụ công việc.

4. Tạo ra, cài đặt, phát tán phần mềm độc hại.

5. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin; ngăn chặn việc truy nhập đến thông tin của cơ quan, cá nhân khác trên môi trường mạng, trừ trường hợp pháp luật cho phép.

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

7. Các hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

Điều 5. Phối hợp với những cơ quan/tổ chức có thẩm quyền

1. Trung tâm Công nghệ thông tin và Truyền thông là đơn vị vận hành các hệ thống thông tin, cơ sở dữ liệu dùng chung đặt tại TTTHDL tỉnh.

2. Trung tâm Công nghệ thông tin và Truyền thông là đầu mối liên hệ, phối hợp các cơ quan, tổ chức có thẩm quyền quản lý về ATTT phục vụ việc bảo đảm an toàn, an ninh mạng cho Hệ thống thông tin TTTHDL tỉnh.

3. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố ATTT:

a) Trung tâm Công nghệ thông tin và Truyền thông:

- Người liên hệ: Ông Trần Trường Giang, Chức vụ: Giám đốc.

+ Số điện thoại: 0911.919.000

+ Email: hotro@angiang.gov.vn

b) Cục An toàn thông tin/Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC)

- Người liên hệ/bộ phận: Phòng Ứng cứu sự cố

+ Số điện thoại: 0869 100 317

+ Email: ir@vncert.vn

+ Báo cáo sự cố qua nền tảng điều phối, xử lý sự cố an toàn thông tin mạng quốc gia: https://irlab.vn

+ Báo cáo sự cố qua website của VNCERT/CC: https://vncert.vn

Điều 6. Bảo đảm nguồn nhân lực

1. Tuyển dụng

Công chức, viên chức được tuyển dụng vào vị trí làm về ATTT có trình độ, chuyên ngành về lĩnh vực CNTT, ATTT, phù hợp với vị trí tuyển dụng.

2. Trong quá trình làm việc

a) Trách nhiệm bảo đảm ATTT đối với người quản lý và vận hành hệ thống:

- Thiết lập phương pháp hạn chế truy cập mạng không dây, giám sát và điều khiển truy cập không dây, tổ chức sử dụng chứng thực và mã hóa để bảo vệ truy cập không dây tới hệ thống thông tin.

- Tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin.

b) Trách nhiệm bảo đảm ATTT đối với người sử dụng hệ thống:

- Có trách nhiệm đảm bảo ATTT đối với từng vị trí công việc.

- Phải thường xuyên tổ chức quán triệt các quy định về ATTT, nhằm nâng cao nhận thức về trách nhiệm đảm bảo ATTT.

- Phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp thiết bị.

c) Định kỳ hàng năm tổ chức hoặc tham gia phổ biến, tuyên truyền nâng cao nhận thức và đào tạo kỹ năng cơ bản về ATTT cho người sử dụng do đơn vị chức năng tổ chức.

3. Chấm dứt thay đổi công việc

a) Công chức, viên chức chấm dứt hoặc thay đổi công việc phải thu hồi tài khoản truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức.

b) Bộ phận chuyên trách thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi công chức, viên chức thôi việc.

c) Lập biên bản bàn giao tài sản và tài khoản CNTT (nếu có).

d) Cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc.

Chương II:
BẢO ĐẢM ATTT TRONG
QUẢN LÝ THIẾT KẾ, XÂY DỰNG HỆ THỐNG

Điều 7. Thiết kế an toàn hệ thống thông tin

Trung tâm Công nghệ thông tin và Truyền thông:

1. Xây dựng tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin.

2. Xây dựng tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.

3. Xây dựng tài liệu mô tả phương án bảo đảm ATTT theo cấp độ.

4. Xây dựng tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm ATTT của hệ thống thông tin thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

5. Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống, báo cáo Lãnh đạo quyết định trước khi thực hiện thay đổi.

Điều 8. Phát triển phần mềm thuê khoán

1. Yêu cầu có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán.

2. Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm.

3. Kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng.

4. Kiểm tra, đánh giá ATTT, trước khi đưa vào sử dụng.

Điều 9. Thử nghiệm và nghiệm thu hệ thống

1. Bên triển khai xây dựng kế hoạch, nội dung, quy trình, có bộ phận chịu trách nhiệm thử nghiệm và nghiệm thu hệ thống.

2. Đơn vị vận hành thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác theo phương án thiết kế được phê duyệt trong Hồ sơ đề xuất cấp độ.

3. Bộ phận chuyên trách và bên triển khai hệ thống xây dựng kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống, có báo cáo nghiệm thu được Chủ quản hệ thống thông tin phê duyệt trước khi đưa hệ thống vào vận hành, khai thác.

4. Bộ phận chuyên trách phối hợp với đơn vị độc lập (bên thứ ba) hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm nghiệm thu hệ thống.

Điều 10. Bảo đảm ATTT khi tiếp nhận, phát triển, vận hành và bảo trì hệ thống thông tin

1. Khi thực hiện nâng cấp, mở rộng, thay thế một phần hệ thống thông tin, phải rà soát cấp độ, phương án bảo đảm an toàn của hệ thống thông tin và thực hiện điều chỉnh, bổ sung hoặc thay mới hồ sơ đề xuất cấp độ trong trường hợp cần thiết.

2. Khi tiếp nhận, phát triển, nâng cấp, bảo trì hệ thống thông tin, đơn vị phải tiến hành phân tích, xác định rủi ro có thể xảy ra, đánh giá phạm vi tác động và phải chuẩn bị các biện pháp hạn chế, loại trừ các rủi ro này và yêu cầu các bên cung cấp, thi công, các cá nhân liên quan thực hiện.

3. Trong quá trình vận hành hệ thống thông tin, đơn vị chủ quản hệ thống thông tin cần thực hiện đánh giá, phân loại hệ thống thông tin theo cấp độ; triển khai phương án bảo đảm an toàn hệ thống thông tin đáp ứng yêu cầu cơ bản trong tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm an toàn hệ thống thông tin theo cấp độ; thường xuyên kiểm tra, giám sát an toàn hệ thống thông tin; tuân thủ quy trình vận hành, quy trình xử lý sự cố đã xây dựng; ghi lại và lưu trữ đầy đủ thông tin nhật ký hệ thống để phục vụ quản lý, kiểm soát thông tin.

4. Các đơn vị trực thuộc Sở Thông tin và Truyền thông, các đơn vị có máy chủ đặt tại TTTHDL phải có trách nhiệm yêu cầu các đối tác (nếu có), tuân thủ các quy định về đảm bảo ATTT của quy chế này đảm bảo ATTT cho toàn bộ he thống TTTHDL, tránh lộ, lọt dữ liệu, tài liệu thiết kế, quản trị hệ thống mà đối tác đang xử lý ra bên ngoài.

Chương III:
BẢO ĐẢM ATTT TRONG QUẢN LÝ VẬN HÀNH HỆ THỐNG

Điều 11. Quản lý an toàn mạng

1. Hoạt động của hệ thống phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của hệ thống.

2. Toàn bộ cấu hình hệ thống phải được sao lưu, dự phòng trên thiết bị hoặc hệ thống lưu trữ độc lập, định kỳ 01 tháng/lần hoặc theo quy định từng nội dung liên quan.

3. Khi thực hiện nâng cấp, thay đổi cấu hình hệ thống phải thực hiện ngoài giờ làm việc.

4. Phải kiểm tra hoạt động tổng thể của hệ thống sau khi thay đổi cấu hình hoặc nâng cấp hệ thống.

5. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố:

a) Định kỳ hàng tháng hoặc khi có thay đổi, bộ phận chuyên trách thực hiện sao lưu, dự phòng hệ thống trên hệ thống độc lập như: ổ cứng di động hoặc SAN, NAS và các thiết bị lưu trữ khác.

b) Các dữ liệu sau yêu cầu sao lưu, dự phòng: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

6. Truy cập và quản lý cấu hình hệ thống:

a) Cấu hình hệ thống từ xa phải sử dụng các giao thức bảo mật có mã hóa thông tin như SSL, TLS, SSH, VPN.

b) Khi cấu hình hệ thống từ bên ngoài phải thông qua kết nối VPN và được mã hóa trên giao thức đường truyền theo đúng các quy định về bảo mật truy cập từ xa.

c) Toàn bộ cấu hình hệ thống phải được lưu trên thiết bị hoặc hệ thống lưu trữ độc lập.

d) Thiết lập, phân quyền đối với các tài khoản truy cập hệ thống và được sự đồng ý từ quản trị hệ thống.

đ) Ghi và lưu trữ nhật ký hệ thống trong thời gian tối thiểu 90 ngày với những thông tin cơ bản: tên tài khoản, địa chỉ, nhật ký hoạt đông và thao tác, các lỗi phát sinh trong quá trình hoạt động,…

Điều 12. Quản lý an toàn máy chủ và ứng dụng

Quy định về quản lý an toàn máy chủ và ứng dụng:

1. Quy định với máy chủ

a) Hoạt động của máy chủ phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của ứng dụng.

b) Ảnh hệ điều hành phải được sao lưu dự phòng trên hệ thống lưu trữ độc lập định kỳ 01 tháng/lần.

c) Máy chủ phải được nâng cấp, xử lý điểm yếu ATTT trên máy chủ trước khi đưa vào sử dụng.

d) Việc kết nối, gỡ bỏ máy chủ khỏi hệ thống phải được sự cho phép của Thủ trưởng đơn vị và xóa sạch dữ liệu.

đ) Có tài liệu liệt kê, cài đặt với những phần mềm hệ thống cài trong máy chủ.

2. Quy định với ứng dụng:

a) Hoạt động của ứng dụng phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của ứng dụng.

b) Ứng dụng phải được thiết lập chính sách xác thực; Kiểm soát truy cập; Có phương án bảo mật thông tin liên lạc và biện pháp bảo đảm an toàn ứng dụng và mã nguồn.

c) Ứng dụng phải được định kỳ kiểm tra đánh giá ATTT tối thiểu 01 năm/lần hoặc khi thay đổi, nâng cấp mở rộng.

3. Truy cập mạng của máy chủ:

a) Kết nối, truy cập máy chủ phải được kiểm soát bởi tường lửa hệ thống.

b) Chỉ mở cổng quản trị hệ thống từ vùng mạng LAN hoặc vùng mạng quản trị (nếu có).

c) Truy cập quản trị máy chủ từ bên ngoài mạng phải qua kênh kết nối VPN. Các máy tính truy cập từ xa phải đảm bảo an toàn bảo mật thông tin trên đường truyền kết nối và cài đặt các phần mềm anti-virus.

d) Phân quyền, quy định thời gian kết nối đối với các tài khoản kết nối.

4. Truy cập và quản trị máy chủ và ứng dụng:

a) Định kỳ từ 03 đến 06 tháng thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng.

b) Chỉ cấp quyền quản lý máy chủ và ứng dụng cho công chức, viên chức quản trị theo chức năng nhiệm vụ được giao.

c) Truy cập quản trị máy chủ và ứng dụng phải qua giao thức mã hóa như SSL, TLS, SSH và VPN.

d) Truy cập quản trị máy chủ và ứng dụng từ bên ngoài mạng phải qua kênh kết nối VPN.

đ) Các máy tính quản trị hệ thống phải cài đặt các phần mềm phòng chống mã độc có bản quyền (anti-virus) và phải quét mã độc trước khi kết nối vào hệ thống.

e) Phần quyền, quy định thời gian kết nối đối với các tài khoản quản trị.

5. Quy định về cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố:

a) Định kỳ hàng tháng hoặc khi nâng cấp ứng dụng phải sao lưu, dự phòng mã nguồn ứng dụng và cơ sở dữ liệu trên thiết bị hoặc hệ thống độc lập.

b) Dữ liệu lưu trữ phải được mã hóa cùng mã kiểm tra tính nguyên vẹn.

c) Dữ liệu lưu trữ phải được quản lý theo phiên bản và có quản lý truy cập.

6. Cấu hình tối ưu và tăng cường bảo mật cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác

a) Kiểm soát và theo dõi tất cả các phương pháp truy cập từ xa tới hệ thống thông tin, triển khai nhiều cơ chế giám sát, cam kết từ các truy cập từ xa; phát hiện sớm việc truy cập trái phép vào mạng máy tính hay thiết bị lưu trữ dữ liệu.

b) Cấu hình hệ thống thông tin 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.

Điều 13. Quản lý an toàn dữ liệu

1. Quy định dự phòng và khôi phục dữ liệu:

a) Định kỳ hàng tuần, tháng phải sao lưu, dự phòng cơ sở dữ liệu và dữ liệu nghiệp vụ (nếu có) trên thiết bị hoặc hệ thống độc lập.

b) Phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau.

2. Định kỳ hàng tháng hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

3. Bản sao lưu được lưu trữ trên thiết bị hoặc hệ thống độc lập.

4. Bố trí máy tính riêng, đặt mật khẩu, mã hóa dữ liệu và các biện pháp bảo mật khác bảo đảm ATTT khi lưu trữ và truy cập cơ sở dữ liệu hệ thống.

5. Nghiêm cấm các hành vi chia sẻ các tài liệu, dữ liệu liên quan đến hệ thống TTTHDL khi chưa được sự cho phép của lãnh đạo, người có thẩm quyền và chưa được mã hóa.

Điều 14. Quản lý an toàn thiết bị đầu cuối

1. Thông tin về thiết bị đầu cuối (tên máy tính, tải khoản, chủng loại, địa chỉ MAC, địa chỉ IP) phải được quản lý và cập nhật.

2. Khi truy cập và sử dụng thiết bị đầu cuối từ xa phải có cơ chế xác thực và sử dụng giao thức mạng an toàn.

3. Việc cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống phải được cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt.

Điều 15. Quản lý phòng chống phần mềm độc hại

1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống mã độc. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin.

2. Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu,…), người sử dụng phải báo trực tiếp cho bộ phận có trách nhiệm để xử lý.

3. Phần mềm ứng dụng trước khi được cài đặt, sử dụng phải được kiểm tra xem có phần mềm độc hại tồn tại hay không? Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng.

4. Định kỳ hàng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống.

Điều 16. Quản lý giám sát an toàn hệ thống thông tin

1. Các hệ thống thông tin đặt tại TTTHDL bắt buộc phải có có chức năng ghi và lưu trữ nhật ký về hoạt động của hệ thống và người sử dụng hệ thống thông tin. Thực hiện việc bảo vệ các chức năng ghi nhật ký và thông tin nhật ký, chống giả mạo, sửa đổi, phá hủy và truy cập trái phép.

2. Chủ quản hệ thống thông có hệ thống đặt tại TTTHDL phải tuân thủ quy định về đảm bảo ATTT tại Quy chế này và phối hợp với Trung tâm Công nghệ thông tin và Truyền thông trong trường hợp xảy ra sự cố liên quan đến vấn đề an toàn, an ninh thông tin hệ thống đang vận hành.

3. Nguyên tắc, yêu cầu, nội dung, phương thức, hệ thống kỹ thuật phục vụ công tác giám sát thực hiện theo đúng quy định tại Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông quy định hoạt động giám sát An toàn hệ thống thông tin và hướng dẫn triển khai theo Công văn số 2973/BTTTT-CATTT ngày 04/9/2019 của Bộ Thông tin và Truyền thông.

4. Đối tượng giám sát về cơ bản bao gồm máy chủ, thiết bị mạng, thiết bị bảo mật, máy chủ, dịch vụ, ứng dụng, các thiết bị đầu cuối và điểm giám sát đường truyền, cụ thể: giám sát lớp mạng, giám sát lớp máy chủ, giám sát lớp ứng dụng và giám sát lớp đầu cuối.

5. Phải đảm bảo được thực hiện thường xuyên, liên tục. Chủ động theo dõi, phân tích, phòng ngừa nhằm kịp thời phát hiện, ngăn chặn rủi ro, sự cố an toàn thông tin mạng.

6. Đảm bảo ổn định, bí mật cho thông tin cung cấp, trao đổi trong quá trình giám sát.

Điều 17. Quản lý điểm yếu ATTT

1. Quản lý thông tin điểm yếu ATTT đối với từng thành phần có trong hệ thống (hệ điều hành, máy chủ, ứng dụng, dịch vụ…); Phân loại mức độ nguy hiểm của điểm yếu; Xây dựng phương án và quy trình xử lý đối với từng mức độ nguy hiểm của điểm yếu.

2. Báo cáo Lãnh đạo/Người quản lý ngay khi phát hiện điểm yếu ATTT ở mức độ nghiêm trọng. Thực hiện cảnh báo và xử lý điểm yếu ATTT theo chỉ đạo. Việc xử lý điểm yếu ATTT phải bảo đảm không làm ảnh hưởng/gián đoạn hoạt động của hệ thống.

3. Xây dựng phương án xử lý tạm thời đối với trường hợp điểm yếu ATTT chưa được khắc phục và phương án khôi phục hệ thống trong trường hợp xử lý điểm yếu thất bại.

4. Có trách nhiệm phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu ATTT đối với các điểm yếu khi cần thiết.

5. Kiểm tra, đánh giá và xử lý điểm yếu ATTT cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng.

6. Định kỳ 01 năm kiểm tra, đánh giá điểm yếu ATTT cho toàn bộ hệ thống thông tin; Thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu ATTT khi có thông tin hoặc nhận được cảnh báo về điểm yếu ATTT đối với thành phần cụ thể trong hệ thống.

Điều 18. Quản lý sự cố ATTT

1. Thực hiện cô lập hệ thống, ngắt kết nối với các hệ thống liên quan khác.

2. Khi có sự cố ATTT xảy ra, bộ phận chuyên trách phải sao lưu, dự phòng toàn bộ hiện trạng hệ thống trước khi xử lý sự cố.

3. Liên hệ với Sở Thông tin và Truyền thông.

Điều 19. Quản lý an toàn người sử dụng đầu cuối

1. Người sử dụng có trách nhiệm tự bảo vệ thông tin cá nhân của mình. Khi sử dụng, khai thác các hệ thống thông tin của cơ quan, đơn vị và các phần mềm ứng dụng dùng chung đặt tại TTTHDL, 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.

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

c) Khi khai thác, sử dụng các phần mềm dùng chung 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 quy định:

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 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 CNTT 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. Các đơn vị thuộc Sở phải thường xuyên kiểm tra, giám sát các hoạt động chia sẻ, gửi, nhận thông tin, dữ liệu trong hoạt động nội bộ của mình. Khuyến cáo việc chia sẻ, gửi, nhận thông tin trên môi trường mạng cần phải sử dụng mật khẩu để bảo vệ thông tin.

4. Đối với hoạt động trao đổi thông tin, dữ liệu với bên ngoài, đơn vị và cá nhân thực hiện trao đổi thông tin, dữ liệu ra bên ngoài cam kết và có biện pháp bảo mật thông tin, dữ liệu được trao đổi.

Điều 20. Quản lý rủi ro an toàn thông tin mạng

Đơn vị vận hành xây dựng và ban hành Hồ sơ Quản lý rủi ro ATTT bao gồm các nội dung sau:

1. Danh mục tài sản thông tin, dữ liệu có trong hệ thống.

2. Đánh giá các rủi ro ATTT đối với mỗi loại tài sản.

3. Có phương án dự phòng và khôi phục sau sự cố đối với thông tin, dữ liệu và ứng dụng.

Việc kiểm tra, đánh giá và quản lý rủi ro cần tuân thủ các nội dung sau:

a) Kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ.

b) Đánh giá hiệu quả của biện pháp bảo đảm an toàn hệ thống thông tin.

c) Đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống.

d) Kiểm tra, đánh giá khác do chủ quản hệ thống thông tin quy định.

Điều 21. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

Quy định, quy trình về Kết thúc vận hành, khai thác, thanh lý, hủy bỏ bao gồm các nội dung sau:

1. Thiết bị CNTT có chứa dữ liệu (máy tính, thiết bị lưu trữ, ...) khi bị hỏng phải được công chức vận hành kiểm tra, sửa chữa, khắc phục. Phải có biện pháp kiểm tra, giám sát đảm bảo không để lọt lộ thông tin hay lây nhiễm mã độc đối với máy tính mang ra bên ngoài sửa chữa, bảo hành.

2. Trước khi tiến hành thanh lý/loại bỏ thiết bị CNTT cũ, phải áp dụng các biện pháp kỹ thuật xoá bỏ hoàn toàn dữ liệu người dùng đã tạo ra, đảm bảo không thể phục hồi.

3. Các phương tiện và thiết bị CNTT: Máy tính cá nhân (PC), máy tính xách tay, máy chủ, các thiết bị mạng, phương tiện lưu trữ như CD/DVD, thẻ nhớ, ổ cứng phải xóa sạch dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng.

Chương IV:
TỔ CHỨC BẢO ĐẢM ATTT

Điều 22. Trách nhiệm của Trung tâm Công nghệ thông tin và Truyền thông

Thực hiện trách nhiệm theo quy định tại Điều 21, Điều 22 Nghị định 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về việc bảo đảm an toàn hệ thống thông tin theo cấp độ.

Điều 23. Trách nhiệm của công chức, viên chức, người lao động thuộc Sở

Thực hiện nghiêm túc các quy định về quản lý, vận hành hệ thống tại đơn vị theo đúng các quy định hiện hành. Chấp hành đúng các quy định về ATTT tại Quy chế này.

Điều 24. Trách nhiệm của các cơ quan, đơn vị, tổ chức có liên quan

Các cơ quan, đơn vị, tổ chức có liên quan khi thuê các dịch vụ phần mềm, cơ sở dữ liệu, hệ thống thông tin, dịch vụ vận hành, đặt chỗ máy chủ tại TTTHDL phải tuân thủ theo các quy định tại quy chế này về quản lý tài khoản, phiên đăng nhập, phân quyền của Trung tâm Công nghệ thông tin và Truyền thông; chịu trách nhiệm với nội dung, dữ liệu hệ thống mình tạo ra, cung cấp phát tán trên môi trường mạng theo quy định pháp luật.

Chương V:
TỔ CHỨC THỰC HIỆN

Điều 25. Rà soát, cập nhật, bổ sung Quy chế

Trung tâm Công nghệ thông tin và Truyền thông:

1. Định kỳ 02 năm hoặc khi có quy định, chính sách mới cần điều chỉnh, bổ sung Quy chế bảo đảm ATTT, Trung tâm Công nghệ thông tin và Truyền thông tham mưu rà soát, cập nhật, bổ sung quy chế phù hợp.

2. Có hồ sơ lưu lại thông tin phản hồi của đối tượng áp dụng chính sách trong quá trình triển khai, áp dụng chính sách ATTT.

3. Phổ biến đến toàn thể công chức, viên chức người lao động thuộc Sở Thông tin và Truyền thông và Cơ quan, tổ chức, cá nhân có kết nối, sử dụng Hệ thống thông tin TTTHDL tỉnh./.