ỦY BAN NHÂN DÂN TỈNH VĨNH LONG	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 333/QĐ-UBND	*Vĩnh Long, ngày 26 tháng 02 năm 2024*

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn thông tin mạng đối với Trung tâm Tích hợp dữ liệu tỉnh Vĩnh Long

CHỦ TỊCH ỦY BAN NHÂN DÂN TỈNH

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19/6/2015; Luật sửa đổi, bổ sung một số điều của Luật Tổ chức Chính phủ và Luật Tổ chức chính quyền địa phương ngày 22/11/2019;

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

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 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 ngày 01/7/2016 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 05/TTr-STTTT ngày 18/01/2024,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin mạng đối với Trung tâm Tích hợp dữ liệu tỉnh Vĩnh Long.

Điều 2. Giao Giám đốc Sở Thông tin và Truyền thông chủ trì hướng dẫn, kiểm tra, đôn đốc các cơ quan, tổ chức, cá nhân trong tỉnh triển khai thực hiện Quyết định này.

Điều 3. Chánh Văn phòng UBND tỉnh, Giám đốc Sở Thông tin và Truyền thông, thủ trưởng các sở, ban, ngành tỉnh, Chủ tịch UBND các huyện, thị xã, thành phố và các cơ quan, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này.

Quyết định có hiệu lực thi hành kể từ ngày ký./.

Nơi nhận:
- Như điều 3;
- CT, PCT.UBND tỉnh phụ trách VX;
- CVP, PVP.UBND tỉnh phụ trách VX;
- Phòng VHXH, TT.THCB, TT.PVHCC;
- Lưu: VT, 3.30.05.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Nguyễn Thị Quyên Thanh

ỦY BAN NHÂN DÂN **TỈNH VĨNH LONG**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**

QUY CHẾ
Quy chế bảo đảm an toàn thông tin mạng đối với Trung tâm Tích hợp dữ liệu tỉnh Vĩnh Long

(Ban hành kèm theo Quyết định số 333/QĐ-UBND ngày 26 tháng 02 năm 2024 của Chủ tịch UBND tỉnh)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi và đối tượng áp dụng

1. Quy chế này quy định việc bảo đảm an toàn thông tin mạng (ATTT) trong quá trình quản lý, vận hành, khai thác, sử dụng các hệ thống thông tin đặt tại Trung tâm Tích hợp dữ liệu tỉnh Vĩnh Long (say đây gọi là Trung tâm dữ liệu).

2. Quy chế này áp dụng đối với cán bộ, công chức, viên chức, người lao động của các cơ quan Nhà nước; các tổ chức, cá nhân có liên quan tham gia vào các hoạt động quản lý, vận hành, khai thác sử dụng, cung cấp hạ tầng, dịch vụ công nghệ thông tin và bảo đảm ATTT cho các hệ thống thông tin đặt tại Trung tâm dữ liệu.

Điều 2. Mục tiêu và 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 các hệ thống thông tin tại Trung tâm dữ liệu.

2. Nguyên tắc

a) Cơ quan, tổ chức, cá nhân thuộc đối tượng áp dụng Quy chế này có trách nhiệm bảo đảm ATTT mạng cho 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 mạng 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 cho các hệ thống thông tin tại Trung tâm dữ liệu 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.

Điều 3. Những hành vi nghiêm cấm

Các hành vi vi phạm theo quy định tại Điều 7 của Luật An toàn thông tin mạng và Điều 8 của Luật an ninh mạng.

Chương II
BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ THIẾT KẾ, XÂY DỰNG HỆ THỐNG

Điều 4. Thiết kế an toàn hệ thống thông tin

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

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

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

4. Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm ATTT.

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.

6. Có phương án quản lý và bảo vệ hồ sơ thiết kế.

7. Có bộ phận chuyên môn đánh giá hồ sơ thiết kế hệ thống thông tin, các biện pháp bảo đảm ATTT trước khi triển khai thực hiện.

Điều 5. Phát triển phần mềm thuê khoán

1. 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 an toàn thông tin, trước khi đưa vào sử dụng;

Điều 6. Thử nghiệm và nghiệm thu hệ thống

Để thực hiện thử nghiệm và nghiệm thu hệ thống trước khi bàn giao và đưa vào sử dụng cần:

1. Thực hiện thử nghiệm và nghiệm thu hệ thống trước khi bàn giao và đưa vào sử dụng;

2. Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống;

3. Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống;

4. Có 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 và nghiệm thu hệ thống;

5. Có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của đơn vị được giao quản lý hệ thống thông tin trước khi đưa vào sử dụng theo quy định.

Chương III
BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ VẬN HÀNH HỆ THỐNG

Điều 7. Quản lý an toàn mạng

1. Quản lý, vận hành hoạt động bình thường của hệ thống

a) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn.

b) Thường xuyên kiểm tra cấu hình, các file nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện và xử lý những sự cố nếu có.

c) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm.

d) Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp.

đ) Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng.

e) Các bản quyền phần mềm cần được thống kê, quản lý thời gian phục vụ cho việc gia hạn.

f) Triển khai hệ thống phát hiện phòng chống xâm nhập giữa các vùng mạng quan trọng.

g) Sử dụng thêm các phương pháp xác thực đa nhân tố đối với các thiết bị mạng quan trọng.

h) Triển khai phương án cảnh báo thời gian thực trực tiếp đến người quản trị hệ thống thông qua hệ thống giám sát khi phát hiện sự cố trên các thiết bị mạng.

i) Duy trì ít nhất 02 kết nối mạng Internet từ các ISP sử dụng hạ tầng kết nối trong nước khác nhau đối với hệ thống buộc phải có kết nối mạng Internet.

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

a) Triển khai hệ thống lưu trữ độc lập với hệ thống lưu trữ của các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

b) Triển khai phương án dự phòng nóng cho các thiết bị mạng chính bảo đảm khả năng vận hành liên tục của hệ thống; năng lực của thiết bị dự phòng phải đáp ứng theo quy mô hoạt động của hệ thống.

c) Triển khai hệ thống lưu trữ nhật ký độc lập và phù hợp với hoạt động của các thiết bị mạng. Dữ liệu nhật ký phải được lưu tối thiểu 03 tháng.

d) Triển khai hệ thống chống thất thoát dữ liệu trong hệ thống.

3. Truy cập và quản lý cấu hình hệ thống

a) Cán bộ quản lý, nhân viên vận hành truy cập, khai thác thông tin tại hệ thống theo trách nhiệm và phân quyền được quy định; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài.

b) Cán bộ quản lý, nhân viên vận hành có trách nhiệm theo dõi và phát hiện các trường hợp truy cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, báo cáo cho cán bộ quản lý để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm.

c) Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác.

d) Quy trình kết nối thiết bị đầu cuối của người sử dụng vào hệ thống mạng; truy nhập và quản lý cấu hình hệ thống; cấu hình tối ưu, tăng cường bảo mật cho thiết bị mạng, bảo mật (cứng hóa) trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác.

đ) Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác.

Điều 8. Quản lý an toàn máy chủ và ứng dụng

1. Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ.

a) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn.

b) Thường xuyên kiểm tra cấu hình, các file nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện và xử lý những sự cố nếu có.

c) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm.

d) Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp.

đ) Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng.

e) Các bản quyền phần mềm cần được thống kê, quản lý thời gian hạn phục vụ cho việc gia hạn.

2. Truy cập mạng của máy chủ

Bảo đảm các kết nối mạng trên máy chủ hoạt động liên tục, ổn định và an toàn. Cấu hình, kiểm soát các kết nối, các cổng dịch vụ từ bên trong đi ra cũng như bên ngoài vào hệ thống.

3. Truy cập và quản trị máy chủ và ứng dụng

a) Thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng.

b) Cấp quyền quản lý truy cập của người sử dụng trên máy chủ cài đặt hệ điều hành.

c) Toàn bộ máy chủ và thiết bị công nghệ thông tin không phải máy tính ngoại trừ các hệ thống bắt buộc phải có giao tiếp với Internet (các hệ thống phục vụ truy cập Internet; cung cấp giao diện ra Internet của trang tin điện tử; phục vụ cập nhật bản vá hệ điều hành, mẫu mã độc, mẫu điểm yếu, mẫu tấn công) không được kết nối Internet.

d) Sử dụng cơ chế xác thực đa nhân tố khi truy cập vào các máy chủ trong hệ thống, các tài khoản quản trị của ứng dụng; có cơ chế yêu cầu người sử dụng thay đổi thông tin xác thực định kỳ.

đ) Kiểm tra tính toàn vẹn của các tệp tin hệ thống và tính toàn vẹn của các quyền đã được cấp trên các tài khoản hệ thống.

e) Sử dụng cơ chế mã hóa thông tin xác thực của người sử dụng/bên sử dụng trước khi gửi đến ứng dụng qua môi trường mạng.

f) Xác thực thông tin, nguồn gửi khi trao đổi thông tin trong quá trình quản trị ứng dụng (không phải là thông tin, dữ liệu công khai) qua môi trường mạng.

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

5. Cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống máy chủ và ứng dụng.

6. Kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống.

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

Điều 9. Quản lý an toàn dữ liệu

1. Yêu cầu an toàn đối với phương pháp mã hóa

a) Đơn vị xây dựng và áp dụng quy định sử dụng các phương thức mã hóa thích hợp theo các chuẩn quốc gia hoặc quốc tế đã được công nhận để bảo vệ thông tin.

b) Phải có biện pháp quản lý khóa mã hóa thích hợp để hỗ trợ việc sử dụng các kỹ thuật mã hóa.

2. Phân loại, quản lý và sử dụng khóa bí mật và dữ liệu mã hóa.

3. Cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu.

4. Trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ.

5. Sao lưu dự phòng và khôi phục dữ liệu (*tần suất sao lưu dự phòng, phương tiện lưu trữ, thời gian lưu trữ; nơi lưu trữ, phương thức lưu trữ và phương thức lấy dữ liệu ra khỏi phương tiện lưu trữ*).

6. Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ.

7. Định kỳ 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 và các thông tin, dữ liệu quan trọng khác trên hệ thống (*nếu có*).

Điều 10. Quản lý an toàn thiết bị đầu cuối

Quy định về quản lý an toàn thiết bị đầu cuối bao gồm các nội dung:

1. Quản lý, vận hành hoạt động bình thường cho thiết bị đầu cuối;

2. Kết nối, truy cập và sử dụng thiết bị đầu cuối từ xa;

3. Cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống;

4. Cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho máy tính người sử dụng và thực hiện quy trình trước khi đưa hệ thống vào sử dụng;

5. Kiểm tra, đánh giá, xử lý điểm yếu ATTT cho thiết bị đầu cuối trước khi đưa vào sử dụng.

Điều 11. Quản lý phòng chống phần mềm độc hại

1. Cài đặt, cập nhật, sử dụng phần mềm phòng chống mã độc; dò quét, kiểm tra phần mềm độc hại trên máy tính, máy chủ và thiết bị di động;

2. Cài đặt, sử dụng phần mềm trên máy tính, thiết bị di động và việc truy cập các trang thông tin trên mạng;

3. Gửi nhận tập tin qua môi trường mạng và các phương tiện lưu trữ di động;

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 12. Quản lý giám sát an toàn hệ thống thông tin

Chính sách, quy trình quản lý giám sát an toàn hệ thống thông tin bao gồm:

1. Quản lý, vận hành hoạt động bình thường của hệ thống giám sát;

2. Đối tượng giám sát bao gồm: thiết bị hệ thống, máy chủ, ứng dụng, dịch vụ và các thành phần khác trong hệ thống;

3. Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát;

4. Truy cập và quản trị hệ thống giám sát;

5. Loại thông tin cần được giám sát;

6. Lưu trữ và bảo vệ thông tin giám sát (nhật ký hệ thống);

7. Đồng bộ thời gian giữa hệ thống giám sát và thiết bị được giám sát;

8. Theo dõi, giám sát và cảnh báo sự cố phát hiện được trên hệ thống thông tin;

9. Bố trí nguồn lực và tổ chức giám sát an toàn hệ thống thông tin 24/7.

Điều 13. Quản lý điểm yếu ATTT

Chính sách, quy trình quản lý điểm yếu ATTT bao gồm:

1. Quản lý thông tin các thành phần có trong hệ thống có khả năng tồn tại điểm yếu ATTT: thiết bị hệ thống, hệ điều hành, máy chủ, ứng dụng, dịch vụ và các thành phần khác.

2. Quản lý, cập nhật nguồn cung cấp điểm yếu ATTT; phân nhóm và mức độ của điểm yếu cho các thành phần trong hệ thống đã xác định.

3. Cơ chế phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu ATTT.

4. 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.

5. 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 14. Quản lý sự cố ATTT

1. Phân nhóm sự cố ATTT mạng theo quy định tại Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm ATTT mạng quốc gia; xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố ATTT mạng, ứng phó sự cố ATTT mạng.

2. Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố ATTT mạng;

3. Kế hoạch ứng phó sự cố ATTT mạng.

4. Giám sát, phát hiện và cảnh báo sự cố ATTT.

5. Quy trình ứng cứu sự cố ATTT mạng thông thường.

6. Quy trình ứng cứu sự cố ATTT mạng nghiêm trọng.

7. Cơ chế phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố ATTT.

8. Định kỳ tổ chức diễn tập phương án xử lý sự cố ATTT.

Điều 15. Quản lý an toàn người sử dụng đầu cuối

Chính sách, quy trình quản lý an toàn người sử dụng đầu cuối bao gồm:

1. Quản lý truy cập, sử dụng tài nguyên nội bộ.

2. Quản lý truy cập mạng và tài nguyên trên Internet.

Điều 16. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

1. Thực hiện các quy định về bảo đảm ATTT khi kết thúc vận hành, khai thác, thanh lý, hủy bỏ.

2. Thực hiện quy trình xử lý thông tin trên hệ thống khi thay đổi mục đích sử dụng hoặc gỡ bỏ.

3. Phương án kỹ thuật thực hiện xử lý thông tin trên hệ thống khi thay đổi mục đích sử dụng hoặc gỡ bỏ.

Chương IV
TỔ CHỨC BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 17. Bảo đảm nguồn nhân lực

1. Tuyển dụng

a) Công chức, viên chức, người lao động được tuyển dụng vào vị trí việc làm về ATTT phải có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, phù hợp với vị trí tuyển dụng theo quy định.

b) Có quy định, quy trình tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ;

c) Có chuyên gia trong lĩnh vực đánh giá, kiểm tra trình độ chuyên môn phù hợp với vị trí tuyển dụng.

2. Trong quá trình làm việc

a) Công chức, viên chức được cấp quyền tham gia vào các hoạt động quản lý, vận hành, truy cập, khai thác sử dụng các hệ thống thông tin tại Trung tâm dữ liệu phải tuân thủ và thực hiện theo nội quy, quy chế bảo đảm Trung tâm dữ liệu.

b) Định kỳ hàng năm, Sở Thông tin và Truyền thông chủ trì, phối hợp các đơn vị liên quan xây dựng kế hoạch và tổ chức triển khai thực hiện phổ biến, tuyên truyền nâng cao nhận thức về ATTT cho người sử dụng; kế hoạch đào tạo về ATTT hàng năm cho 03 nhóm đối tượng bao gồm: công chức, viên chức quản lý, vận hành kỹ thuật và người sử dụng trong hệ thống.

3. Chấm dứt thay đổi công việc

a) Công chức, viên chức quản lý, vận hành hệ thống khi chấm dứt hoặc thay đổi công việc phải thu hồi các quyền truy cập hệ thống, 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 cơ quan, tổ chức.

b) Thực hiện quy trình vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi công chức, viên chức đã thôi việc.

c) Có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc.

Điều 18. Trách nhiệm của Sở Thông tin và Truyền thông

1. Định kỳ rà soát, cập nhật Quy chế đúng với thực tế triển khai và phù hợp với các quy định của pháp luật.

2. Vận hành Trung tâm dữ liệu hoạt động ổn định và bảo đảm ATTT; bảo đảm các yêu cầu về hạ tầng kỹ thuật, chất lượng dịch vụ, triển khai đầy đủ các phương án bảo đảm ATTT theo quy định.

3. Định kỳ rà soát, cập nhật hồ sơ cấp độ phù hợp với thực tế và các quy định của pháp luật, hướng dẫn của cơ quan chuyên ngành.

4. Hướng dẫn các tổ chức, cá nhân có liên quan thực hiện Quy chế này khi tham gia quản trị, vận hành, khai thác, sử dụng; cung cấp hạ tầng, dịch vụ công nghệ thông tin và bảo đảm ATTT tại Trung tâm dữ liệu.

5. Phối hợp các đơn vị liên quan xây dựng hồ sơ đề xuất cấp độ ATTT đối với các hệ thống thông tin được cài đặt, vận hành tại Trung tâm dữ liệu.

6. Ban hành các biểu mẫu, quy định có liên quan đến quản lý, vận hành, bảo đảm ATTT tại Trung tâm dữ liệu.

Điều 19. Trách nhiệm của đơn vị vận hành hệ thống thông tin

Các cơ quan, đơn vị có hệ thống thông tin cài đặt, vận hành tại Khu vực đặt máy chủ dùng riêng của Trung tâm dữ liệu có trách nhiệm:

1. Thực hiện nghiêm các quy định trong Quy chế này; tuân thủ và thực hiện đúng các quy định các quy định liên quan ATTT.

2. Kiểm tra, bảo đảm ATTT theo quy định đối với các máy chủ, thiết bị, ứng dụng CNTT của đơn vị trước khi cài đặt, vận hành tại Trung tâm dữ liệu.

3. Có trách nhiệm bố trí kinh phí đầu tư, nâng cấp, bảo đảm ATTT và bảo trì, bảo dưỡng đối với các máy chủ, thiết bị, ứng dụng CNTT của đơn vị đã cài đặt, vận hành tại Trung tâm dữ liệu nhằm đảm bảo hệ thống hoạt động ổn định và liên tục.

4. Phối hợp với Sở Thông tin và Truyền thông kiểm soát, phát hiện và khắc phục các sự cố mất ATTT; định kỳ đánh giá ATTT theo quy định của pháp luật.

5. Cử công chức, viên chức, người lao động tham gia đầy đủ các hội nghị, hội thảo, các khóa đào tạo, bồi dưỡng về an toàn, an ninh thông tin do tỉnh hoặc cơ quan chuyên ngành tổ chức.

Điều 20. Trách nhiệm của đơn vị quản lý hệ thống thông tin

Các cơ quan, đơn vị có hệ thống thông tin cài đặt tại Khu vực đặt máy chủ dùng chung của Trung tâm dữ liệu có trách nhiệm:

1. Tổ chức tuyên truyền, phổ biến cho toàn bộ công chức, viên chức và người lao động của đơn vị biết quy chế này để nâng cao nhận thức về an toàn, an ninh thông tin; thực hiện đúng các quy định nêu tại Quy chế này.

2. Phối hợp với Sở Thông tin và Truyền thông kiểm soát, phát hiện và khắc phục các sự cố mất ATTT.

3. Cử công chức, viên chức, người lao động tham gia đầy đủ các hội nghị, hội thảo, các khóa đào tạo, bồi dưỡng về an toàn, an ninh thông tin do tỉnh hoặc cơ quan chuyên ngành tổ chức.

4. Tổ chức thực hiện các Điều 6, Điều 7, Điều 8 Quy chế này.

Điều 21. Trách nhiệm của cá nhân

1. Cá nhân phụ trách ATTT có trách nhiệm

a) Chấp hành nghiêm và chịu trách nhiệm triển khai các giải pháp kỹ thuật, quy trình bảo đảm ATTT được quy định tại Quy chế này.

b) Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm tra, phát hiện và khắc phục các sự cố mất ATTT.

c) Thường xuyên học tập nghiên cứu, cập nhật, nâng cao kiến thức, kinh nghiệm, trình độ chuyên môn đáp ứng tốt các yêu cầu về bảo đảm ATTT theo quy định.

d) Tham gia đầy đủ các chương trình đào tạo, tập huấn về ATTT do Tỉnh hoặc các bộ, ngành Trung ương tổ chức.

2. Cá nhân là người sử dụng có trách nhiệm

a) Chấp hành nghiêm túc các quy định tại Quy chế này trong quá trình truy cập, khai thác dữ liệu được vận hành tại Trung tâm dữ liệu.

b) Nâng cao ý thức cảnh giác và trách nhiệm đảm bảo ATTT trong phạm vi trách nhiệm và quyền hạn được giao.

c) Tự quản lý, chịu trách nhiệm bảo quản an toàn thông tin đối với các tài khoản, mật khẩu được giao, cấp phát sử dụng; không cung cấp, chia sẻ tài khoản, mật khẩu cho bất kỳ cá nhân, tổ chức khác khi chưa có sự đồng ý của đơn vị quản lý hệ thống thông tin.

d) Khi phát hiện các dấu hiệu bị lộ lọt thông tin tài khoản, mật khẩu hoặc sự cố mất ATTT phải báo ngay với cấp Lãnh đạo đơn vị, bộ phận chuyên trách ATTT của đơn vị và Sở Thông tin và Truyền thông để phối hợp ngăn chặn, xử lý kịp thời.

đ) Tham gia đầy đủ các chương trình đào tạo, tập huấn về ATTT do Tỉnh hoặc các bộ, ngành Trung ương tổ chức.

Điều 22. Phối hợp với những cơ quan/tổ chức có thẩm quyền

1. Sở Thông tin và Truyền thông có trách nhiệm làm đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về ATTT

a) Quản lý về ATTT phục vụ việc bảo đảm an toàn, an ninh mạng cho các hệ thống thông tin tại Trung tâm dữ liệu.

b) Tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về ATTT mạng của các hệ thống thông tin tại Trung tâm dữ liệu.

c) Hỗ trợ điều phối xử lý sự cố ATTT mạng. Tùy theo mức độ sự cố, phối hợp với các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố ATTT mạng.

2. Các cơ quan, đơn vị có liên quan tham gia các hoạt động, công tác bảo đảm ATTT khi có yêu cầu của Sở Thông tin và Truyền thông hoặc các cơ quan, tổ chức có thẩm quyền.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 23. Sở Thông tin và Truyền thông

1. Chủ trì tổ chức thực hiện các nhiệm vụ được giao tại Quy chế này.

2. Tuyên truyền, phổ biến, hướng dẫn việc thực hiện các quy định của Quy chế này đến các cơ quan Nhà nước, cán bộ, công chức, viên chức và tổ chức, cá nhân có liên quan đến quản lý, vận hành, sử dụng các ứng dụng, dịch vụ tại Trung tâm dữ liệu.

3. Định kỳ hàng năm hoặc đột xuất thực hiện tổng hợp, báo cáo UBND tỉnh về tình hình quản lý, vận hành và bảo đảm ATTT tại Trung tâm dữ liệu.

Điều 24. Công an tỉnh

Phối hợp Sở Thông tin và Truyền thông bảo đảm an toàn thông tin cho Trung tâm dữ liệu; kiểm tra an toàn thông tin đối với các máy chủ, thiết bị và ứng dụng CNTT của các cơ quan Nhà nước trước khi cài đặt vận hành tại Trung tâm dữ liệu.

Điều 25. Sở Tài chính

Chủ trì, phối hợp với Sở Thông tin và Truyền thông tham mưu, trình UBND tỉnh phê duyệt kinh phí hàng năm đảm bảo thực hiện tốt nhiệm vụ bảo đảm ATTT đối với Trung tâm dữ liệu.

Điều 26. Các sở, ban, ngành tỉnh; UBND huyện, thị xã, thành phố và các tổ chức, cá nhân có liên quan

1. Trong phạm vi chức năng, nhiệm vụ của mình, có trách nhiệm tổ chức triển khai và kiểm tra chấp hành tại đơn vị theo đúng Quy chế này.

2. Bảo đảm ATTT đối với máy chủ, thiết bị và ứng dụng CNTT theo quy định trước khi cài đặt, vận hành tại Trung tâm dữ liệu.

3. Chủ trì, phối hợp với Sở Thông tin và Truyền thông triển khai các giải pháp bảo đảm ATTT, đánh giá an toàn thông tin và khắc phục sự cố đối với hệ thống thông tin của đơn vị được cài đặt, vận hành tại Trung tâm dữ liệu đảm bảo thực hiện kịp thời, nhanh chóng và hiệu quả.

4. Định kỳ trước ngày 30 tháng 11 hằng năm báo cáo về Sở Thông tin và Truyền thông tình hình thực hiện công tác bảo đảm ATTT trong quá trình quản lý, vận hành, khai thác, sử dụng các ứng dụng, dịch vụ của đơn vị được cài đặt tại Trung tâm dữ liệu.

Điều 27. Khen thưởng và xử lý vi phạm

1. Cơ quan, đơn vị, tổ chức, cá nhân thực hiện tốt Quy chế này và có sáng kiến, giải pháp kỹ thuật đảm bảo an toàn, an ninh thông tin đem lại hiệu quả tốt, thiết thực sẽ được xem xét đánh giá khen thưởng.

2. Trường hợp vi phạm Quy chế này thì tùy theo tính chất, mức độ vi phạm sẽ bị xử lý, kỷ luật theo quy định của pháp luật.

Điều 28. Xây dựng và công bố

1. Quy chế này được xây dựng, lấy ý kiến các cơ quan Nhà nước, đơn vị có liên quan trước khi ban hành và công bố áp dụng.

2. Tổ chức tuyên truyền, phổ biến đến cán bộ công chức, viên chức trong Nhà nước trên địa bàn tỉnh biết để thực hiện; thông báo cho các cơ quan, đơn vị có liên quan biết để phối hợp thực hiện.

Điều 29. Rà soát, cập nhật, bổ sung Quy chế

1. Định kỳ 02 năm hoặc khi có thay đổi chính sách ATTT kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung Quy chế này.

2. Lập hồ sơ lưu lại thông tin phản hồi của đối tượng thực hiện quy chế này trong quá trình triển khai, áp dụng.

Trong quá trình triển khai thực hiện Quy chế, nếu có khó khăn, vướng mắc hoặc có vấn đề phát sinh, các cơ quan, đơn vị kịp thời phản ánh về Sở Thông tin và Truyền thông để tổng hợp, tham mưu, trình Chủ tịch UBND tỉnh điều chỉnh, bổ sung đảm bảo phù hợp với các quy định hiện hành./