| | |
|---|---|
| UBND TỈNH BÌNH ĐỊNH<br>**THANH TRA TỈNH** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**<br>**Độc lập – Tự do – Hạnh phúc** |
| Số: 187 /QĐ-TTT | *Bình Định, ngày 14 tháng 10 năm 2024* |

# QUYẾT ĐỊNH
## Về việc ban hành Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống thông tin Thanh tra tỉnh

## CHÁNH THANH TRA

*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 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 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;*

*Căn cứ Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 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;*

*Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;*

*Căn cứ Quyết định số 22/2021/QĐ-UBND ngày 11 tháng 6 năm 2021 của UBND tỉnh Bình Định về việc ban hành Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Bình Định;*

*Căn cứ Quyết định số 10/2024/QĐ-UBND ngày 19 tháng 4 năm 2024 của UBND tỉnh ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Thanh tra tỉnh;*

*Theo đề nghị của Chánh Văn phòng Thanh tra tỉnh.*

## QUYẾT ĐỊNH:

**Điều 1.** Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn, an ninh mạng Hệ thống thông tin Thanh tra tỉnh.

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

**Điều 3.** Chánh Văn phòng, Trưởng các phòng, công chức, người lao động thuộc Thanh tra tỉnh và các cơ quan, đơn vị, tổ chức cán bộ, công chức, cá nhân liên quan chịu trách nhiệm thi hành Quyết định này./.

***Nơi nhận:***
- Như Điều 3:
- CTT, các PCTT;
- Lưu: VT, VP.

**CHÁNH THANH TRA**

CỘNG HÒA XHCN VIỆT NAM
THANH TRA VIỆT NAM
THANH TRA TỈNH BÌNH ĐỊNH

**Nguyễn Văn Thơm**

Số: 187/QĐ-TTT
Thời gian ký: 2024-10-31T14:28:32+07:00



# QUY CHẾ

## Bảo đảm an toàn, an ninh mạng Hệ thống thông tin Thanh tra tỉnh

*(Ban hành kèm theo Quyết định số: 187 /QĐ-TTT ngày 14 tháng 10 năm 2024 của Thanh tra tỉnh Bình Định)*

## Chương I:
## QUY ĐỊNH CHUNG

### Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Phạm vi điều chỉnh

Quy chế này quy định về đảm bảo an toàn thông tin cho các Hệ thống thông tin của Thanh tra tỉnh Bình Định.

2. Đối tượng áp dụng

a. Các phòng thuộc Thanh tra tỉnh Bình Định; các cán bộ, công chức và người lao động ở các phòng thuộc Thanh tra tỉnh Bình Định và các đối tượng tham gia vận hành, khai thác các hệ thống thông tin của Thanh tra tỉnh.

b. Cơ quan, tổ chức, cá nhân có kết nối, sử dụng các hệ thống thông tin của Thanh tra tỉnh.

c. Cơ quan, tổ chức, cá nhân cung cấp dịch vụ quản lý, vận hành, duy trì, phát triển và bảo đảm an toàn thông tin mạng phục vụ hoạt động cho các Hệ thống thông tin của Thanh tra 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 số và các 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. *An ninh mạng* là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

3. *Bảo vệ an ninh mạng* là phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm an ninh mạng.

4. *Không gian mạng* là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, 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.

5. *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.

6. *Môi trường mạng* là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua cơ sở hạ tầng thông tin.

7. *Hệ thống thông tin* là tập hợp thiết bị 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 như: Hệ thống mạng nội bộ, hệ thống văn phòng điện tử, hệ thống thư điện tử, trang thông tin điện tử, hệ thống camera giám sát,…

8. *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.

9. *Tấn công mạng* là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để phá hoại, gây gián đoạn hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử.

10. *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.

11. *Đơn vị vận hành hệ thống thông tin* là cơ quan, tổ chức được chủ quản hệ thống thông tin giao nhiệm vụ vận hành hệ thống thông tin.

12. *Tài khoản số* là thông tin dùng để chứng thực, xác thực, phân quyền sử dụng các ứng dụng, dịch vụ trên không gian mạng.

13. *Xâm phạm an toàn thông tin mạng* là hành vi truy nhập, sử dụng, tiết lộ, làm gián đoạn, sửa đổi, phá hoại trái phép thông tin, hệ thống thông tin.

14. *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.

15. *Rủi ro an toàn thông tin mạng* là những nhân tố chủ quan hoặc khách quan có khả năng ảnh hưởng tới trạng thái an toàn thông tin mạng.

16. *Đánh giá rủi ro* an toàn thông tin mạng là việc phát hiện, phân tích, ước lượng mức độ tổn hại, mối đe dọa đối với thông tin, hệ thống thông tin.

17. *Quản lý rủi ro* an toàn thông tin mạng là việc đưa ra các biện pháp nhằm giảm thiểu rủi ro an toàn thông tin mạng.

18. *Hạ tầng kỹ thuật* là tập hợp các thiết bị tính toán, lưu trữ, thiết bị ngoại vi, thiết bị kết nối mạng, thiết bị phụ trợ, đường truyền, mạng nội bộ, mạng diện rộng,..

**Điều 3. Mục tiêu, nguyên tắc bảo đảm an toàn thông tin**

1. Mục tiêu bảo đảm an toàn thông tin

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 của Thanh tra tỉnh.

2. Nguyên tắc

a. Bảo đảm an toàn, an ninh thông tin là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt quá trình liên quan đến thông tin và thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ hệ thống thông tin. Bảo đảm an toàn, an ninh thông tin tuân thủ các nguyên tắc chung quy định tại Điều 4 Luật An toàn thông tin mạng và Điều 4 Nghị định số 85/2016/NĐ-CP.

b. Các phòng, cá nhân thuộc cơ quan có trách nhiệm bảo đảm an toàn, an ninh thông tin mạng; bố trí nhân sự phụ trách chịu trách nhiệm bảo đảm an toàn, an ninh thông tin mạng; xác định rõ quyền hạn, trách nhiệm của từng bộ phận, cá nhân trong cơ quan đối với công tác bảo đảm an toàn, an ninh thông tin mạng.

c. Công chức, viên chức và người lao động trong cơ quan có trách nhiệm bảo đảm an toàn, an ninh thông tin trong phạm vi xử lý công việc của mình theo quy định của Nhà nước, của ngành và các quy định liên quan.

d. Thông tin mật, thông tin thuộc Danh mục bí mật nhà nước phải được bảo vệ theo quy định của Nhà nước, quy định của cơ quan về công tác bảo vệ bí mật Nhà nước và các nội dung tương ứng trong Quy chế này.

đ. 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, cá nhân liên quan và theo quy định của pháp luật.

**Điều 4. Những hành vi nghiêm cấm**

1. Các hành vi bị nghiêm cấm quy định tại Điều 7 và Điều 8 của Luật An toàn thông tin 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; tự ý thay đổi các cài đặt hệ thống mạng của cơ quan.

3. Tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin cài đặt trên thiết bị công nghệ thông tin 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. Lãnh đạo Thanh tra tỉnh giao Văn phòng là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin phục vụ việc bảo đảm an toàn, an ninh mạng cho các Hệ thống thống thông tin Thanh tra tỉnh.

2. Văn phòng làm đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin: Tùy theo mức độ sự cố, phối hợp với các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin mạng.

3. Các phòng, cá nhân trực thuộc cơ quan tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của các cơ quan, tổ chức có thẩm quyền.

**Điều 6. Bảo vệ bí mật nhà nước trong ứng dụng công nghệ thông tin**

1. Quy định về soạn thảo, in ấn, phát hành và sao chụp tài liệu mật

a. Không được sử dụng máy tính nối mạng (Internet và nội bộ) để soạn thảo văn bản, chuyển giao, lưu trữ thông tin có nội dung bí mật nhà nước; không được cung cấp tin, bài, tài liệu và đưa thông tin bí mật nhà nước lên Trang tin điện tử/cổng Thông tin điện tử. Nghiêm cấm cài cắm các thiết bị lưu trữ tài liệu có nội dung bí mật nhà nước vào máy tính nối mạng Internet.

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

2. Khi máy tính dùng để soạn thảo văn bản mật có sự cố, các phòng, cá nhân phải báo cho Văn phòng để xử lý theo quy định. Không được tự ý sửa chữa hoặc cho phép cá nhân, tổ chức không có trách nhiệm trực tiếp sửa chữa, xử lý và khắc phục các sự cố của máy tính dùng để soạn thảo văn bản mật. Đối với các máy tính để soạn thảo văn bản mật phải xây dựng nội quy, quy định quản lý sử dụng đảm bảo theo quy định của Luật bảo vệ bí mật nhà nước hiện hành.

3. Trước khi thanh lý các máy tính trong đơn vị, cán bộ chuyên trách/bán chuyên trách công nghệ thông tin phải tiêu huỷ dữ liệu trong ổ cứng máy tính. Không được thanh lý ổ cứng máy tính dùng soạn thảo và chứa các nội dung mật.

**Điều 7. Bảo đảm nguồn nhân lực**

Bố trí công chức vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp.

a. Có quy định về việc thực hiện nội quy, quy chế bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống;

b. Có kế hoạch và định kỳ hàng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng;

c. Thường xuyên cử cán bộ, công chức tham gia đào tạo, bồi dưỡng về an toàn thông tin hàng năm cho 03 nhóm đối tượng bao gồm: cán bộ phụ trách, cán bộ quản lý và người sử dụng trong hệ thống.

d. Khi chấm dứt, thay đổi công việc phải xác định rõ trách nhiệm của cá nhân và các bên liên quan trong quản lý, sử dụng các tài sản công nghệ thông tin được giao, phải thay đổi hoặc thu hồi quyền truy cập các hệ thống thông tin.

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

### Điều 8. 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 an toàn thông tin theo cấp độ

4. Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin.

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, tổ chuyên gia đánh giá hồ sơ thiết kế hệ thống thông tin, các biện pháp bảo đảm an toàn thông tin trước khi triển khai thực hiện.

### Điều 9. Quản lý thuê dịch vụ công nghệ thông tin, 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.

5. Khi thay đổi mã nguồn, kiến trúc phần mềm thực hiện kiểm tra, đánh giá an toàn thông tin cho phần mềm.

6. Có cam kết của bên phát triển về bảo đảm tính bí mật và bản quyền của phần mềm phát triển.

### Điều 10. Thử nghiệm và nghiệm thu hệ thống

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 chủ quản hệ thống thông tin trước khi đưa vào sử dụng.

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

### Điều 11. Quản lý an toàn mạng

1. Quản lý hạ tầng mạng nội bộ:

a) Tuân thủ các quy định kiến trúc hệ thống, tiêu chuẩn, quy chuẩn kỹ thuật; cài đặt, cấu hình, tổ chức hệ thống mạng phù hợp với các tiêu chuẩn ứng dụng công nghệ thông tin của các cơ quan nhà nước, bảo đảm an toàn thông tin; hạn chế sử dụng mô hình mạng có nguy cơ mất an toàn thông tin cao;

b) Tổ chức mô hình mạng: Trang bị thiết bị tường lửa chuyên dụng hoặc phần mềm tường lửa để ngăn chặn và phát hiện xâm nhập trái phép vào mạng nội bộ của cơ quan, đơn vị khi kết nối với hệ thống bên ngoài; Xây dựng hoặc thuê hệ thống giám sát an toàn thông tin để kiểm soát, phát hiện truy cập trái phép vào hệ thống.

c) Đối với các phòng không nằm cùng một khu vực thì cần thiết lập mạng riêng ảo (VPN) để tăng cường an ninh cho hạ tầng mạng nội bộ. Khi thiết lập các dịch vụ trên môi trường mạng Internet, chỉ cung cấp những chức năng thiết yếu nhất bảo đảm duy trì hoạt động của hệ thống thông tin; hạn chế sử dụng/mở cổng giao tiếp mạng, giao thức và các dịch vụ không cần thiết.

d) Khi thực hiện truy nhập từ xa vào mạng nội bộ thực hiện chức năng quản trị, phải sử dụng giao thức mạng có mã hóa thông tin (như: SSL/TLS, VPN...) và thiết lập mật khẩu có độ phức tạp cao..

đ) Xây dựng 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 trong hệ thống và thực hiện quy trình trướckhi đưa hệ thống vào vận hành khai thác.

e). Không tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập không dây của cá nhân vào mạng nội bộ cơ quan, đơn vị.

g) Không tự ý thay đổi, gỡ bỏ biện pháp, giải pháp an toàn thông tin cài đặt trên thiết bị công nghệ thông tin phục vụ công việc; tự ý thay thế, lắp mới, tráo đổi thành phần của máy tính phục vụ công việc. Cá nhân, tổ chức phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng.

2. Quản lý hệ thống mạng không dây.

a) Khi thiết lập mạng không dây để kết nối với mạng cục bộ thông qua các điểm truy nhập (Access Point - AP), cơ quan, đơn vị vận hành phải thiết lập các tham số: Tên, nhận dạng dịch vụ (Service Set Identifier - SSID), mật khẩu có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặc biệt như: !, @, #, $, %).

b) Mật khẩu đăng nhập phải được thiết lập có độ phức tạp cao, định kỳ 6 tháng thay đổi mật khẩu nhằm tăng cường công tác bảo mật.

c) Khi cung cấp truy cập Internet qua mạng không dây cho người ngoài, cơ quan, đơn vị vận hành phải tạo thêm một SSID riêng và giới hạn băng thông truy cập phù hợp đối với đối tượng này.

2. Bảo đảm an toàn thông tin khi sử dụng máy tính

a. Cán bộ, công chức và người lao động chỉ cài đặt phần mềm hợp lệ và thuộc danh mục phần mềm được phép sử dụng do cơ quan có thẩm quyền ban hành trên máy tính được đơn vị cấp cho mình; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của lãnh đạo đơn vị; thường xuyên cập nhật phần mềm và hệ điều hành; Khóa màn hình máy tính khi rời khỏi bàn làm việc. Đăng xuất khỏi hệ thống, ứng dụng khi ngừng sử dụng. Tắt máy sau mỗi buổi làm việc.

b. Cài đặt phần mềm xử lý phần mềm độc hại và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính phải tắt máy và báo trực tiếp cho cán bộ chuyên trách/bán chuyên trách về công nghệ thông tin để được xử lý kịp thời.

c. Cán bộ, công chức và người lao động chỉ được sử dụng máy tính vào các hoạt động nghiệp vụ. Không sử dụng máy tính để truy cập, tải về, lưu trữ, phát tán những nội dung vi phạm pháp luật; Không tự tiện thay đổi cấu hình, phần cứng của máy tính được trang bị; Việc sử dụng thiết bị lưu trữ di động như ổ cứng di động, ổ USB, ...: Chỉ sử dụng thiết bị lưu trữ di động cho các hoạt động nghiệp vụ, quản lý khi được sự đồng ý của Lãnh đạo cơ quan; Thực hiện các biện pháp bảo đảm an ninh, an toàn cho thiết bị lưu trữ di động như quét mã độc định kỳ, mã hóa dữ liệu.

3. Truy cập và quản lý cấu hình hệ thống

a. Cán bộ quản lý, 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 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 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 trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác.

4. Quản lý về cấp phát, thu hồi, cập nhật và quản lý các tài khoản truy cập vào hệ thống thông tin

a. Trách nhiệm, quyền hạn người dùng khi truy cập, đăng nhập các hệ thống thông tin, đảm bảo mỗi người dùng khi sử dụng hệ thống thông tin phải được cấp và sử dụng tài khoản truy cập với định danh duy nhất gắn với người dùng đó. Trường hợp sử dụng tài khoản dùng chung cho một nhóm người hay một đơn vị, phải có cơ chế xác định các cá nhân, đơn vị có trách nhiệm quản lý tài khoản. Người dùng chỉ được truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình và có trách nhiệm bảo mật tài khoản truy cập được cấp.

b. Cán bộ chuyên trách thực hiện quản lý, cấp tài khoản cá nhân và phân quyền truy cập cho người sử dụng trên tất cả các máy trạm đặt tại các cơ quan, đơn vị. Trong trường hợp cần thiết có thể hủy tài khoản truy cập cá nhân và ngắt kết nối đối với các hành vi cố ý tấn công hoặc gây trở ngại cho mạng máy tính; hủy quyền truy cập hệ thống thông tin đối với cán bộ, công chức (CBCC) nghỉ chế độ, chuyển công tác. Hướng dẫn người sử dụng thay đổi mật khẩu ngay sau khi đăng nhập lần đầu tiên và bảo vệ thông tin của tài khoản theo quy định.

c. Mật mã đăng nhập, truy cập hệ thống thông tin phải có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặc biệt như !, @, #, $, %,...).

**Điều 12. Quản lý an toàn dữ liệu**

Bảo đảm an toàn thông tin mức dữ liệu

a. Cơ quan thực hiện bảo vệ thông tin, dữ liệu liên quan đến hoạt động công vụ, thông tin có nội dung quan trọng, không phải là thông tin công khai bằng các biện pháp như: thiết lập phương án bảo đảm tính bí mật, nguyên vẹn và khả dụng của thông tin, dữ liệu, ...

b. Văn phòng bố trí máy tính riêng không kết nối mạng, đặt mật khẩu, mã hóa dữ liệu và các biện pháp bảo mật khác bảo đảm an toàn thông tin để soạn thảo, lưu trữ dữ liệu, thông tin và tài liệu quan trọng ở các mức độ mật, tuyệt mật, tối mật.

c. Các phòng thuộc cơ quan 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.

d. Đối với hoạt động trao đổi thông tin, dữ liệu với bên ngoài, các phòng 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. Giao dịch trực tuyến phải được truyền đầy đủ, đúng địa chỉ, tránh bị sửa đổi, tiết lộ hoặc nhân bản một cách trái phép; sử dụng các cơ chế xác thực mạnh, chữ ký số khi tham gia giao dịch, sử dụng các giao thức truyền thông an toàn.

**Điều 13. Quản lý an toàn thiết bị đầu cuối**

1. Cán bộ phụ trách công nghệ thông tin có trách nhiệm quản lý các thiết bị công nghệ thông tin phục vụ công việc, hoạt động chung của cơ quan.

2. Công chức và người lao động có trách nhiệm sử dụng và bảo quản các thiết bị công nghệ thông tin được cấp để phục vụ công việc hàng ngày.

3. Trang thiết bị công nghệ thông tin có lưu trữ dữ liệu, tài liệu khi thay đổi mục đích sử dụng hoặc thanh lý, phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó đảm bảo không có khả năng phục hồi.

4. Thiết bị công nghệ thông tin có bộ phận lưu trữ dữ liệu khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài hoặc ngừng sử dụng phải tháo bộ phận lưu trữ khỏi thiết bị hoặc xóa thông tin, dữ liệu lưu trữ trên thiết bị (trừ trường hợp để khôi phục dữ liệu).

**Điều 14 . 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:

a. Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin và các quy định của cơ quan, tổ chức.

b. Khi cài đặt, kết nối máy tính/thiết bị đầu cuối phải thực hiện theo hướng dẫn/quy trình dưới sự giám sát của bộ phận chuyên trách về an toàn thông tin.

c. Máy tính/thiết bị đầu cuối phải được xử lý điểm yếu an toàn thông tin, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống.

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

a. Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao.

b. Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng.

c. Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý.

**Điều 15. 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 16. 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 (tường lửa), ứng dụng, dịch vụ, hệ thống camera giám sát và các thành phần khác trong hệ thống (nếu có);

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 17. Quản lý sự cố an toàn thông tin**

Ngay sau khi phân loại được sự cố, cán bộ phụ trách có trách nhiệm báo cáo Lãnh đạo cơ quan để xem xét loại sự cố và tuỳ theo đối tượng sẽ tiến hành xử lý.

- Trường hợp sự cố được phân loại thông thường thì cơ quan tự triển khai theo phương án ứng cứu sự cố an toàn thông tin mạng thông thường theo quy trình ứng cứu sự cố thông thường của Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 và báo cho Đội ứng cứu sự cố an toàn thông tin mạng (qua Sở Thông tin và Truyền thông) để phối hợp xử lý.

- Trường hợp sự cố được phân loại nghiêm trọng thì gửi báo cáo sự cố đến Đội ứng cứu sự cố an toàn thông tin mạng (qua Sở Thông tin và Truyền thông) đồng thời thực hiện xử lý theo Phương án số 645/PA-TTT ngày 30/8/2023 của

Thanh tra tỉnh về Phương án phối hợp ứng phó sự cố, đảm bảo an toàn thông tin mạng trong hoạt động của Thanh tra tỉnh.

**Điều 18. Đảm bảo an toàn thông tin cho hệ thống camera giám sát**

1. Cơ quan, cá nhân phải đảm bảo an toàn, an ninh thông tin và tuân thủ theo các quy định pháp luật cho hệ thống camera giám sát.

2. Bộ phận quản lý, vận hành hệ thống camera có trách nhiệm phân công cán bộ phụ trách quản trị hệ thống của đơn vị mình; quản lý, lưu trữ bảo mật và thường xuyên thay đổi mật khẩu tài khoản quản trị. Việc cấp, quản lý tài khoản truy cập vào các hệ thống camera thuộc quản lý của đơn vị phải phù hợp với chức năng, nhiệm vụ và phân quyền của từng đối tượng sử dụng.

3. Việc chia sẻ, sử dụng dữ liệu hệ thống camera giám sát phải đảm bảo tính kịp thời, chính xác, khách quan, minh bạch, đúng mục đích, đúng chức năng, nhiệm vụ, quyền hạn của cơ quan, đơn vị. Đồng thời phải đảm bảo các yếu tố bảo mật thông tin, dữ liệu.

4. Khi triển khai đầu tư, lắp đặt, nâng cấp các hệ thống camera phải thực hiện theo đúng các tiêu chuẩn, hướng dẫn kỹ thuật hiện hành; Sử dụng camera giám sát đáp ứng các yêu cầu về bảo đảm ATTT mạng theo quy định; không sử dụng camera giám sát không có chứng nhận xuất xứ, chất lượng sản phẩm hoặc đã được cơ quan có thẩm quyền cảnh báo không bảo đảm ATTT mạng.

5. Về xác định cấp độ cho các hệ thống thông tin có sử dụng camera giám sát phụ thuộc vào việc xác định loại hình hệ thống thông tin, các đơn vị thực hiện theo hướng dẫn của Cục An toàn Thông tin - Bộ Thông tin và Truyền thông tại Văn bản số 294/CATTT-ATHTTT ngày 13/3/2023.

6. Triển khai đầy đủ phương án bảo đảm an toàn theo quy định cho các hệ thống thông tin có sử dụng camera giám sát đang vận hành.

7. Bộ tiêu chí và Quy chuẩn kỹ thuật quốc gia về yêu cầu an toàn thông tin mạng cơ bản cho camera giám sát, các đơn vị áp dụng theo quy định của Bộ Thông tin và Truyền thông.

**Điều 19. Quản lý rủi ro an toàn thông tin**

1. Nhận diện rủi ro

Thường xuyên kiểm tra rủi ro có thể xảy ra đối với hệ thống thông tin bao gồm rủi ro về tấn công mạng, dữ liệu mất an toàn, lỗi do con người, nhận thức sai về an toàn thông tin.

2. Quy trình đánh giá và quản lý rủi ro.

a. Định kỳ đánh giá rủi ro an toàn thông tin mạng. Việc đánh giá rủi ro an toàn thông tin mạng phải do tổ chức chuyên môn được cơ quan nhà nước có thẩm quyền chỉ định thực hiện;

b. Có cơ chế phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục rủi ro an toàn thông tin;

c. Định kỳ 1 năm kiểm tra, đánh giá điểm yếu an toàn thông tin cho toàn bộ hệ thống thông tin; thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin khi có thông tin hoặc nhận được cảnh báo về điểm yếu an toàn thông tin đối với thành phần cụ thể trong hệ thống.

3. Biện pháp kiểm soát rủi ro.

Trên cơ sở đánh giá và quản lý rủi ro, cơ quan cần rà soát, bổ sung các yêu cầu an toàn (biện pháp kiểm soát rủi ro) cho phù hợp với yêu cầu thực tế.

**Điều 20. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ**

1. Thực hiện hủy bỏ toàn bộ thông tin, dữ liệu trên hệ thống với sự xác nhận của đơn vị chủ quản hệ thống thông tin khi kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin. Trong trường hợp thông tin, dữ liệu của hệ thống thông tin lưu trữ trên tài sản vật lý, đơn vị chủ quản hệ thống thông tin thực hiện các biện pháp tiêu hủy hoặc xóa thông tin bảo đảm không có khả năng phục hồi. Với trường hợp đặc biệt không thể tiêu hủy thông tin, dữ liệu thì sử dụng biện pháp tiêu hủy cấu trúc phần lưu trữ dữ liệu trên tài sản đó.

2. Đối với các hệ thống thông tin có dữ liệu được lưu trữ trên tài sản vật lý cần phải mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài thì phải được sự phê duyệt của cấp có thẩm quyền và thực hiện các biện pháp bảo vệ dữ liệu; có cam kết bảo mật thông tin giữa bên có dữ liệu và bên cung cấp dịch vụ sửa chữa thiết bị lưu trữ dữ liệu.

## Chương IV

## KIỂM TRA ĐÁNH GIA CÔNG TÁC ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

**Điều 21. Kế hoạch kiểm tra hằng năm**

1. Văn phòng chủ trì, phối hợp với các phòng thuộc cơ quan tiến hành kiểm tra công tác đảm bảo an toàn thông tin đối với các phòng theo Kế hoạch công tác hằng năm.

2. Tiến hành kiểm tra đột xuất các tại các phòng khi có dấu hiệu vi phạm an toàn đối với các hệ thống thông tin tại phòng.

**Điều 22. Nội dung hình thức kiểm tra đánh giá hệ thống thông tin**

1. Nội dung kiểm tra, đánh giá

a) Kiểm tra việc thực theo các nội dung theo Quy chế này; việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin; kiểm tra hiệu quả của các biện pháp bảo đảm an toàn thông tin;

b) Đánh giá hiệu quả của biện pháp bảo đảm an thông tin tại phòng; phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống;

c) Kiểm tra, đánh giá các nội dung khác theo quy định hệ thống an toàn thông tin.

2. Hình thức kiểm tra, đánh giá

a) Kiểm tra, đánh giá định kỳ theo kế hoạch Thanh tra tỉnh và đơn vị chuyên trách về an toàn thông tin của tỉnh;

b) Kiểm tra, đánh giá đột xuất theo yêu cầu của cấp có thẩm quyền.

## Chương V

## TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG VÀ TỔ CHỨC THỰC HIỆN

### Điều 23. Trách nhiệm của các cơ quan vận hành hệ thống thông tin

1. Trưởng các phòng thuộc Thanh tra tỉnh có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trong công tác bảo đảm an toàn thông tin mạng của đơn vị mình theo quy định tại Luật An toàn thông tin mạng và các văn bản hướng dẫn thi hành Luật An toàn thông tin mạng.

2. Phân công cán bộ chuyên trách bảo đảm an toàn thông tin của đơn vị; chỉ đạo công chức nghiêm túc chấp hành các quy định về bảo đảm an toàn thông tin; tạo điều kiện để các cán bộ phụ trách an toàn thông tin được học tập, nâng cao trình độ về an toàn thông tin; thường xuyên tổ chức quán triệt các quy định về an toàn thông tin trong cơ quan, đơn vị; xác định các yêu cầu, trách nhiệm bảo đảm an toàn thông tin đối với các vị trí cần tuyển dụng hoặc phân công.

3. Thực hiện bảo đảm an toàn thông tin gồm các nội dung cơ bản như quy định về quản lý hạ tầng mạng, bảo đảm an toàn dữ liệu, bảo đảm an toàn thiết bị và người dùng đầu cuối phù hợp với Quy chế này và các quy định của pháp luật.

4. Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố xảy ra một cách kịp thời, nhanh chóng và đạt hiệu quả.

5. Phối hợp chặt chẽ với Công an tỉnh, Sở Thông tin và Truyền thông và các cơ quan, đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin trên không gian mạng.

6. Hàng năm bố trí kinh phí cho việc ứng dụng công nghệ thông tin nói chung và công tác bảo đảm an toàn thông tin mạng nói riêng trong nội bộ cơ quan; lập kế hoạch mua phần mềm chống virus có bản quyền...nhằm thực hiện tốt công tác bảo mật, bảo đảm an toàn thông tin mạng đưa vào dự toán chi để triển khai thực hiện.

7. Phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin.

8. Định kỳ hàng năm hoặc khi có thay đổi chính sách an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung Quy chế bảo đảm an toàn thông tin. 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 an toàn thông tin.

9. Thực hiện các báo cáo về an toàn thông tin mạng khi được Sở Thông tin và Truyền thông yêu cầu.

**Điều 24. Trách nhiệm của cán bộ, công chức trong cơ quan, đơn vị**

1. Trách nhiệm của cán bộ phụ trách về an toàn thông tin/công nghệ thông tin tại cơ quan, đơn vị:

a) Chịu trách nhiệm bảo đảm an toàn thông tin mạng của cơ quan, đơn vị;

b) Tham mưu lãnh đạo cơ quan ban hành các quy chế, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin mạng;

c) Thực hiện việc giám sát, đánh giá, báo cáo Thủ trưởng cơ quan, đơn vị các rủi ro mất an toàn thông tin mạng và mức độ nghiêm trọng của các rủi ro đó;

d) Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn thông tin mạng;

đ) Thường xuyên cập nhật nâng cao kiến thức, trình độ chuyên môn đáp ứng yêu cầu bảo đảm an toàn thông tin mạng của đơn vị.

2. Trách nhiệm của người sử dụng:

a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao;

b) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng;

c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý;

d) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được cơ quan hoặc đơn vị chuyên môn tổ chức.

**Điều 25. Trách nhiệm của các tổ chức, cá nhân liên quan**

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

**Điều 26. Tổ chức thực hiện**

1. Căn cứ Quy chế này, Trưởng các phòng thuộc Thanh tra tỉnh có trách nhiệm tổ chức triển khai thực hiện Quy chế này trong phạm vi quản lý của mình.

2. Văn phòng có trách nhiệm theo dõi, đôn đốc, kiểm tra, đánh giá việc thực hiện Quy chế và thực hiện việc báo cáo về an toàn thông tin mạng khi được Sở Thông tin và Truyền thông yêu cầu.

3. Trong quá trình thực hiện quy chế này, nếu có khó khăn, vướng mắc hoặc phát sinh vấn đề mới, các đơn vị, cá nhân có liên quan phản ánh kịp thời cho lãnh đạo Thanh tra tỉnh (qua Văn phòng) để hướng dẫn, bổ sung điều chỉnh phù hợp./.