ỦY BAN NHÂN DÂN TỈNH BẮC NINH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 22 /2024/QĐ-UBND	*Bắc Ninh, ngày 05 tháng 9 năm 2024*

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan Nhà nước trên địa bàn tỉnh Bắc Ninh

ỦY BAN NHÂN DÂN TỈNH BẮC NINH

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19 tháng 6 năm 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 tháng 11 năm 2019;

Căn cứ Luật ban hành văn bản quy phạm pháp luật ngày 22 tháng 6 năm 2015; Luật sửa đổi, bổ sung một số điều của Luật ban hành văn bản quy phạm pháp luật ngày 18 tháng 6 năm 2020;

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

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan Nhà nước;

Căn cứ Nghị định số 72/2013/NĐ-CP ngày 15 tháng 7 năm 2013 của Chính phủ về việc ban hành Nghị định quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng;

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

Căn cứ Quyết định số 08/2023/QĐ-TTg ngày 05 tháng 4 năm 2023 của Thủ tướng Chính phủ về việc ban hành Quyết định về Mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước;

Căn cứ các Thông tư của Bộ trưởng Bộ Thông tin và Truyền thông: số 27/2017/TT-BTTTT ngày 20 tháng 10 năm 2017 quy định về quản lý, vận hành, kết nối, sử dụng và bảo đảm An toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước; số 12/2019/TT-BTTTT ngày 05 tháng 11 năm 2019 về sửa đổi, bổ sung một số điều của Thông tư số 27/2017/TT-BTTTT ngày 20 tháng 10 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về quản lý, vận hành, kết nối, sử dụng và bảo đảm An toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước; số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 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 báo kết luận số 117/TB-UBND ngày 20 tháng 8 năm 2024 của Chủ tịch UBND tỉnh thông báo kết luận phiên họp UBND tỉnh thường kỳ tháng 8 năm 2024;

Theo đề nghị của Sở Thông tin và Truyền thông tại Tờ trình số 29/TTr-STTTT ngày 08 tháng 8 năm 2024.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Bắc Ninh.

Điều 2. Quyết định này có hiệu lực kể từ ngày 18 tháng 9 năm 2024.

Quyết định này thay thế Quyết định số 21/2019/QĐ-UBND ngày 22 tháng 10 năm 2019 của UBND tỉnh về việc ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước trên địa bàn tỉnh Bắc Ninh.

Điều 3. Thủ trưởng các cơ quan: Văn phòng UBND tỉnh, các sở, ban, ngành, UBND các huyện, thị xã, thành phố và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ Thông tin và Truyền thông (b/c);
- Vụ pháp chế, Cục ATTT - Bộ TTTT;
- Cục Kiểm tra văn bản QPPL- Bộ Tư pháp;
- TTTU, TT HĐND tỉnh (b/c);
- Chủ tịch, các Phó Chủ tịch UBND tỉnh;
- VPTU, VP Đoàn ĐBQH&HĐND tỉnh;
- Cổng TTĐT tỉnh (đăng công báo);
- VPUBND tỉnh: LĐVP, XDCB, HCTC;
- Lưu: VT.

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Lê Xuân Lợi

ỦY BAN NHÂN DÂN
TỈNH BẮC NINH

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

QUY CHẾ

Bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Bắc Ninh

(Ban hành kèm theo Quyết định số: 22/2024/QĐ-UBND ngày 05/9/2024 của UBND tỉnh Bắc Ninh)

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 các chính sách quản lý và các biện pháp nhằm bảo đảm an toàn thông tin của các cơ quan nhà nước trên địa bàn tỉnh Bắc Ninh.

2. Đối tượng áp dụng

Quy chế này áp dụng đối với các sở, ban, ngành, đơn vị thuộc UBND tỉnh; UBND các huyện, thị xã, thành phố; UBND các xã, phường, thị trấn; các đơn vị sự nghiệp sử dụng ngân sách nhà nước; các cơ quan Trung ương trên địa bàn tỉnh, các tổ chức chính trị - xã hội được ngân sách nhà nước bảo đảm kinh phí hoạt động có sử dụng các hệ thống thông tin do UBND tỉnh triển khai và các tổ chức, cá nhân liên quan đến hoạt động ứng dụng công nghệ thông tin (sau đây gọi tắt là CNTT) của các cơ quan nhà nước tỉnh Bắc Ninh (sau đây gọi tắt là cơ quan, đơn vị); cán bộ, công chức, viên chức, người lao động, đang làm việc tại các cơ quan, đơn vị nêu trên.

Điều 2. Giải thích từ ngữ

Theo các văn bản pháp luật hiện hành, các từ ngữ dưới đây được hiểu như sau:

1. *Bảo đảm an toàn thông tin mạng* là việc 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. *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.

3. *Chính sách an toàn thông tin là* các quy tắc, quy trình cho tất cả các tổ chức, cá nhân truy cập và sử dụng tài nguyên trong hệ thống thông tin của tổ chức nhằm bảo đảm tính an toàn cho hệ thống thông tin và chống lại các hoạt động tấn công của tội phạm.

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. *Ứng cứu các sự cố an toàn thông tin mạng* là hoạt động nhằm xử lý, khắc

phục sự cố gây mất an toàn thông tin mạng gồm: theo dõi, thu thập, phân tích, phát hiện, cảnh báo, kiểm tra, xác minh sự cố, ngăn chặn sự cố, khôi phục dữ liệu và khôi phục hoạt động bình thường của hệ thống thông tin.

7. *Lỗ hổng bảo mật (Security vulnerability)* là điểm yếu về an toàn thông tin (sau đây gọi tắt là ATTT) trên phần mềm hoặc phần cứng, bị tin tặc khai thác để truy cập trái phép vào hệ thống thông tin.

8. *Phần mềm độc hại (virus)* 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. *Phần mềm diệt virus* là phần mềm có tính năng phát hiện, loại bỏ các virus máy tính, khắc phục (một phần hoặc hoàn toàn) hậu quả của virus gây ra và có khả năng được nâng cấp để nhận biết các loại virus mới.

10. *Mạng riêng ảo (Virtual Private Network - VPN)* là dịch vụ mạng dùng riêng để kết nối máy tính của các cơ quan, đơn vị hoặc máy tính cá nhân truy cập vào mạng nội bộ để bảo đảm an toàn an ninh thông tin trên đường truyền.

11. *Tường lửa (Firewall)* là hệ thống an ninh mạng, có thể là phần cứng hoặc phần mềm, sử dụng các quy tắc để kiểm soát lưu lượng truy cập (traffic) vào, ra hệ thống.

12. *Hệ thống phát hiện xâm nhập (Intrusion Detection System - IDS)* là phần mềm ứng dụng hoặc thiết bị được xây dựng để giám sát lưu lượng mạng, đồng thời cảnh báo mỗi khi có các hành vi bất thường xâm nhập vào hệ thống.

13. *Hệ thống ngăn ngừa xâm nhập (Intrusion Prevention System - IPS)* là hệ thống phát hiện xâm nhập ngoài khả năng theo dõi, giám sát thì còn có chức năng ngăn chặn kịp thời các hoạt động xâm nhập không mong muốn đối với hệ thống thông tin.

14. *Dịch vụ an toàn thông tin mạng* là dịch vụ bảo vệ thông tin, hệ thống thông tin.

15. *Vùng mạng nội bộ (Local Area Network - LAN)* là vùng mạng đặt các thiết bị mạng, máy trạm và máy chủ dùng trong khu vực giới hạn nhất định, tốc độ truyền tải cao.

16. *Vùng mạng biên* được thiết kế để kết nối hệ thống thông tin ra các mạng bên ngoài và mạng Internet; bảo vệ hệ thống thông tin từ bên ngoài Internet.

17. *Vùng mạng DMZ (Demilitarized Zone – DMZ)* là vùng mạng trung lập giữa mạng nội bộ và mạng Internet, là nơi chứa các thông tin cho phép người dùng từ Internet truy xuất vào và chấp nhận các rủi ro tấn công từ Internet. Các dịch vụ thường được triển khai trong vùng DMZ là: máy chủ Web, máy chủ Mail, máy chủ DNS, máy chủ FTP, …

18. *Vùng máy chủ nội bộ* đặt các máy chủ nội bộ, cung cấp các dịch vụ nội bộ cho người sử dụng trong hệ thống.

19. *Mật khẩu mạnh là* mật khẩu bao gồm chữ hoa, chữ thường, số, ký tự đặc biệt (!,@,#,$,...) có độ dài 8 ký tự trở lên.

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

1. Bảo đảm an toàn thông tin mạng 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, 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 ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Cơ quan, tổ chức, cá nhân có trách nhiệm bảo đảm ATTT mạng. Hoạt động ATTT mạng của cơ quan, tổ chức, cá nhân phải đúng các quy định của pháp luật liên quan.

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

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

5. Phải có phương án tổ chức sao lưu dữ liệu dự phòng cho mọi dữ liệu quan trọng của tỉnh, của cơ quan, đơn vị mình. Lãnh đạo cơ quan, đơn vị phải chịu trách nhiệm nếu để xảy ra mất mát dữ liệu do không tiến hành sao lưu dự phòng.

6. Các thiết bị viễn thông, máy tính trong cơ quan nhà nước khi kết nối đến mạng truyền số liệu chuyên dùng của tỉnh phải tuân thủ theo Điều 8, Quyết định số 08/2023/QĐ-TTg ngày 05/4/2023 của Thủ tướng Chính phủ về việc ban hành Quyết định về Mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước.

Điều 4. Những hành vi nghiêm cấm

1. Các hành vi bị nghiêm cấm quy định tại Điều 7 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; trên cùng một thiết bị thực hiện đồng thời truy cập vào mạng nội bộ và truy cập Internet bằng thiết bị kết nối Internet của cá nhân (modem quay số, USB 3G/4G, điện thoại di động, máy tính bảng, máy tính xách tay).

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. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin:

a) UBND tỉnh giao Sở Thông tin và Truyền thông 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 thông tin mạng cho các hệ thống thông tin do UBND tỉnh

làm chủ quản.

b) Sở Thông tin và Truyền thông làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng theo Quyết định số 2164/QĐ-UBND ngày 08/11/2023 của Chủ tịch UBND tỉnh Bắc Ninh về việc ban hành Quy chế hoạt động của Đội Ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh Bắc Ninh.

2. 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 đảm nguồn nhân lực

1. Tuyển dụng

a) Cán bộ được tuyển dụng 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 với vị trí tuyển dụng.

b) Quy trình tuyển dụng cán bộ, điều kiện tuyển dụng cán bộ và các quy trình đánh giá, kiểm tra trình độ chuyên môn tuân theo các quy định liên quan.

2. Trong quá trình làm việc

a) Đối với người dùng cuối :

- Có trách nhiệm tuân thủ các quy định, hướng dẫn bảo đảm ATTT và các quy định của pháp luật, bảo đảm ATTT đối với từng vị trí công việc;

- Thông báo ngay cho đơn vị chủ quản hệ thống thông tin khi nghi ngờ hoặc phát hiện sự cố, hiện tượng bất thường của hệ thống thông tin;

- Tham gia đầy đủ các lớp tập huấn, đào tạo và tự cập nhật kiến thức về an toàn thông tin mạng;

- Chịu trách nhiệm quản lý, sử dụng trang thiết bị CNTT được giao, bảo đảm ATTT; không được giao cho các tổ chức, cá nhân khác sử dụng trang thiết bị CNTT đã được giao sử dụng; không được sử dụng trang thiết bị CNTT cá nhân để kết nối, truy cập vào các hệ thống thông tin nội bộ nếu chưa được phép của đơn vị chủ quản; không tự thay thế, lắp mới, tráo đổi thành phần của máy tính công vụ; không mang tài sản CNTT của đơn vị ra ngoài nếu chưa được phép của thủ trưởng đơn vị; có trách nhiệm bàn giao cho đơn vị quản lý các trang thiết bị CNTT khi chuyển công tác, thay đổi vị trí việc làm hoặc nghỉ việc.

b) Định kỳ hàng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng.

c) Định kỳ hàng năm tổ chức đào tạo hoặc cử đi đào tạo về an toàn thông tin hàng năm cho 03 nhóm đối tượng bao gồm: cán bộ kỹ thuật, cán bộ quản lý và người sử dụng trong hệ thống.

Các đơn vị liên quan có trách nhiệm phối hợp với Sở Thông tin và Truyền thông xây dựng, triển khai kế hoạch đào tạo, bồi dưỡng, tập huấn về công tác bảo đảm ATTT, an ninh mạng cho đội ngũ công chức, viên chức của cơ quan, đơn vị.

3. Chấm dứt thay đổi công việc

a) Công chức, viên chức, người lao động nghỉ việc hoặc thay đổi công việc phải tuân thủ:

- Phải bàn giao lại công việc, tài khoản truy cập hệ thống thông tin, tài sản CNTT của cơ quan, đơn vị; phải có cam kết giữ bí mật thông tin liên quan đến tổ

chức sau khi nghỉ việc;

- Quản trị viên hệ thống phải vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi công chức, viên chức, người lao động thôi việc.

b) Quy trình 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, người lao động thôi việc:

- Thu hồi tài khoản truy cập, các trang thiết bị máy móc, phần cứng và các tài sản khác thuộc sở hữu của đơn vị quản lý;

- Vô hiệu hóa các thông tin của công chức, viên chức, người lao động thôi việc được lưu trên các phương tiện lưu trữ, phần mềm;

- Vô hiệu hóa tất cả các quyền truy cập của công chức, viên chức, người lao động thôi việc vào tài nguyên, hệ thống phần mềm của đơn vị quản lý;

- Kiểm tra lại các quyền ra vào, truy cập tài nguyên, quản trị hệ thống đã cấp cho công chức, viên chức, người lao động thôi việc để bảo đảm đã hoàn toàn được gỡ bỏ khỏi hệ thống.

c) Cán bộ, công chức, viên chức nghỉ việc hoặc thay đổi công việc phải có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc. Các thông tin bắt buộc cần giữ bí mật, tối thiểu bao gồm:

- Không tiết lộ thông tin được tiếp xúc trong quá trình công tác tại đơn vị cho các cá nhân, tổ chức gây ảnh hưởng bất lợi đến lợi ích của đơn vị;

- Không sử dụng các thông tin được tiếp xúc trong quá trình công tác tại đơn vị vào mục đích trục lợi cá nhân.

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

Điều 7. Thiết kế an toàn hệ thống thông tin trong hồ sơ thiết kế

1. Khi thiết kế, xây dựng hệ thống thông tin phải mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin:

a) Tài liệu phân tích lựa chọn kiến trúc, công nghệ.

b) Tài liệu thiết kế tổng thể hệ thống thể hiện thiết kế hạ tầng và kết nối các thành phần của hệ thống.

c) Các vùng mạng trong hệ thống: Vùng mạng nội bộ; vùng mạng biên; vùng mạng DMZ; vùng máy chủ nội bộ; vùng mạng không dây (nếu có) tách riêng, độc lập với các vùng mạng khác; vùng mạng máy chủ cơ sở dữ liệu; vùng quản trị; vùng quản trị thiết bị hệ thống.

d) Các giải pháp, thiết bị của hệ thống thông tin đáp ứng các quy định của Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ (Thông tư số 12/2022/TT-BTTTT).

2. Khi thiết kế, xây dựng hệ thống thông tin phải mô tả "Kiến trúc hệ thống" trong đó có mô tả thiết kế và các thành phần của hệ thống thông tin thông qua một số mô hình kiến trúc khác nhau nhằm mô tả hệ thống dưới nhiều góc nhìn khác

nhau, bao gồm:

a) Thiết kế kiến trúc ứng dụng.

b) Thiết kế kiến trúc dữ liệu.

c) Thiết kế kiến trúc vật lý.

3. Khi thiết kế, xây dựng hệ thống thông tin phải mô tả phương án bảo đảm an toàn thông tin theo từng cấp độ tương ứng với hồ sơ đề xuất cấp độ được quy định tại Thông tư số 12/2022/TT-BTTTT.

4. Khi thiết kế, xây dựng hệ thống thông tin phải mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin, trong đó cần bảo đảm các tiêu chí:

a) Bảo đảm có từ 2 - 3 công nghệ được phân tích và đưa ra phương án lựa chọn.

b) Phân tích các ưu, nhược điểm của từng công nghệ để từ đó chọn ra công nghệ áp dụng phù hợp nhất.

5. Khi có thay đổi thiết kế, cần đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống

Khi có thay đổi thiết kế, đơn vị được giao chủ trì cần phối hợp với các đơn vị liên quan đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn thông tin mạng đặt ra đối với hệ thống, xây dựng lại hồ sơ đề xuất cấp độ cho hệ thống và trình cấp có thẩm quyền thẩm định, phê duyệt theo quy định

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

a) Hồ sơ thiết kế không được tùy tiện cung cấp cho cá nhân, đơn vị khác không có đủ thẩm quyền.

b) Hồ sơ thiết kế được bảo quản, lưu trữ theo quy định.

Điều 8. Phát triển phần mềm thuê khoán

1. Đối với các nội dung liên quan đến việc phát triển phần mềm thuê khoán, nhà phát triển phải bảo đảm có các cam kết bảo đảm ATTT

2. Nhà phát triển phải cung cấp mã nguồn sản phẩm cho đơn vị thuê theo hình thức ghi đĩa DVD hoặc USB; yêu cầu DVD, USB cần phải đặt mật khẩu để bảo đảm ATTT; Mã nguồn đã được nhà phát kiểm thử nội bộ trước khi bàn giao.

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

Phần mềm phải được kiểm thử tại ít nhất một đơn vị thụ hưởng trước khi nghiệm thu, bàn giao đưa vào khai thác, sử dụng.

4. Cam kết bảo đảm tính bí mật của mã nguồn và bản quyền của phần mềm phát triển

a) Bên phát triển phải có cam kết về bảo đảm tính bí mật của mã nguồn, không cung cấp cho bên thứ 3.

b) Các cá nhân tham gia phát triển, triển khai hệ thống thông tin phải ký biên bản cam kết bảo mật ATTT.

Điều 9. Thử nghiệm và nghiệm thu hệ thống

Hoạt động thử nghiệm và nghiệm thu hệ thống thực hiện theo hướng dẫn tại Thông tư số 24/2020/TT-BTTTT ngày 09/9/2020 của Bộ trưởng Bộ Thông tin và Truyền thông về việc ban hành Thông tư quy định về công tác triển

khai, giám sát công tác triển khai và nghiệm thu dự án đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước.

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

Điều 10. 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.

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

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

i) 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.

k) Duy trì ít nhất 02 kết nối mạng Internet từ các ISP sử dụng hạ tầng kết nối trong nước khác nhau (nếu 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/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên 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/phương tiện 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 06 tháng.

d) Triển khai hệ thống/phương tiện 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) 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.

Điều 11. Quản lý an toàn máy chủ và ứng dụng

1. Quy định với máy chủ

a) Hệ thống máy chủ phải có tính năng sẵn sàng cao, cơ chế dự phòng linh hoạt để bảo đảm hoạt động liên tục.

b) Có biện pháp bảo vệ, dự phòng, phòng chống các nguy cơ do mất cắp, cháy nổ, ngập lụt, động đất và các thảm họa khác do thiên nhiên hoặc con người gây ra và các phương án khôi phục sau thảm họa cho hệ thống máy chủ.

c) Máy chủ phải được thiết lập chính sách xác thực; kiểm soát truy cập; kết nối về hệ thống giám sát tập trung; thực hiện biện pháp phòng chống xâm nhập; phòng chống phần mềm độc hại và xử lý dữ liệu trên máy chủ khi chuyển giao.

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

đ) Việc kết nối, gỡ bỏ máy chủ khỏi hệ thống phải được sự cho phép của thủ trưởng đơn vị và thực hiện theo quy trình đã được phê duyệt.

e) Phần mềm hệ điều hành cài lên máy chủ ưu tiên là phần mềm hệ điều hành có bản quyền hoặc phần mềm mã nguồn mở được sử dụng rộng rãi trong nước và quốc tế.

g) Người quản trị chỉ được cấp quyền truy cập vào các máy chủ có thẩm quyền. Để được cấp tài khoản quản trị phải gửi công văn xin cấp bao gồm các thông tin tối thiểu: Tên, căn cước công dân, số điện thoại, phòng ban đơn vị công tác, mục đích, phạm vi máy chủ cần truy cập... và được phê duyệt bởi đơn vị quản lý hệ thống thông tin.

h) Ghi nhật ký, quy định thời gian về hoạt động tác động vào các máy chủ, người sử dụng, lỗi phát sinh và các sự cố nhằm trợ giúp cho việc điều tra giám sát về sau.

2. Quy định với ứng dụng

a) Các yêu cầu, thiết kế về an toàn bảo mật của phần mềm ứng dụng cần được xác định rõ trong tài liệu phân tích, thiết kế. Trong quá trình triển khai, vận hành các phần mềm ứng dụng cần bảo đảm nghiêm ngặt theo các yêu cầu, thiết kế về an toàn bảo mật.

b) Ứng dụng phải được thiết lập chính sách xác thực; kiểm soát truy cập; kết nối về hệ thống giám sát tập trung; có phương án bảo mật thông tin liên lạc, chống chối bỏ và biện pháp bảo đảm an toàn ứng dụng và mã nguồn.

c) Có phương án xác định và khắc phục rủi ro trước, trong quá trình triển khai và khi vận hành các phần mềm ứng dụng.

d) Ứng dụng phải kiểm tra, thử nghiệm và có biên bản đánh giá tính an toàn, bảo mật đối với phần mềm ứng dụng theo yêu cầu khi nghiệm thu các phần mềm này. Việc tiến hành thử nghiệm phải bảo đảm trên môi trường riêng biệt, không ảnh hưởng tới hoạt động và dữ liệu của đơn vị.

đ) Quản lý và phân quyền truy cập phần mềm ứng dụng và cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ của người sử dụng. Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của nhân viên và phải được phê duyệt từ cấp trên.

3. Quy định với ứng dụng thư điện tử

a) Không sử dụng các hộp thư điện tử công cộng trong công việc; không sử dụng thư điện tử công vụ vào mục đích cá nhân.

b) Mỗi cá nhân cần đặt mật khẩu đủ mạnh cho hộp thư điện tử của mình.

c) Khi công chức, viên chức, người lao động nghỉ việc thì hộp thư điện tử sẽ bị khóa và xóa bỏ khỏi hệ thống thư điện tử.

d) Đơn vị quản lý hệ thống thư điện tử cần xây dựng phương án bảo đảm an toàn và tính khả dụng truy cập cho hệ thống thư điện tử trong nội bộ và trên Internet, phương án chống thư rác cho thư điện tử.

đ) Bảo đảm an toàn cho hệ thống thư điện tử: Thực hiện theo hướng dẫn tại công văn số 430/BTTTT-CATTT ngày 09 tháng 2 năm 2015 của Bộ Thông tin và Truyền thông về việc hướng dẫn bảo đảm an toàn thông tin cho hệ thống thư điện tử của cơ quan, tổ chức nhà nước.

4. Quy định đối với Cổng, trang thông tin điện tử

a) Quản lý toàn bộ các phiên bản của mã nguồn, tổ chức mô hình Cổng, trang thông tin điện tử hợp lý, tránh khả năng tấn công leo thang đặc quyền. Yêu cầu hệ thống thông tin của Cổng, trang thông tin điện tử phải có các hệ thống phòng vệ như tường lửa, thiết bị phát hiện, phòng chống xâm nhập (IDS/IPS), tường lửa web (WAP- Web Application Firewall).

b) Cổng, trang thông tin điện tử khi đưa vào sử dụng hoặc khi bổ sung thêm các chức năng mới cần đánh giá kiểm định nhằm tránh được các lỗi bảo mật thường xảy ra trên ứng dụng web như: SQL Injection, Cross-Site Scripting (xss),...

c) Xây dựng phương án sao lưu, phục hồi Cổng, trang thông tin điện tử, trong đó chú ý mỗi tháng thực hiện việc sao lưu dữ liệu toàn bộ nội dung Cổng, trang thông tin điện tử một lần bao gồm mã nguồn, cơ sở dữ liệu, dữ liệu phi cấu trúc,... để bảo đảm khi có sự cố có thể khắc phục lại ngay trong vòng 24 giờ.

d) Bảo đảm an toàn cho Cổng, trang thông tin điện tử: Thực hiện theo hướng dẫn tại công văn số 2132/BTTTT-VNCERT ngày 18 tháng 7 năm 2011 của Bộ Thông tin và Truyền thông về việc hướng dẫn bảo đảm an toàn thông tin cho các Cổng, trang thông tin điện tử.

Điều 12. Quản lý an toàn dữ liệu

1.Thực hiện quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn.

2. Có cơ chế sao lưu dữ liệu dự phòng, lưu trữ dữ liệu tại nơi an toàn đồng thời thường xuyên kiểm tra để bảo đảm sẵn sàng phục hồi nhằm ngăn ngừa và hạn chế khi sự cố ATTT mạng xảy ra.

3. Tiến hành cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ được thực hiện theo yêu cầu của đơn vị vận hành hệ thống.

4. Sử dụng mật mã để bảo đảm an toàn và bảo mật dữ liệu trong lưu trữ.

5. Quản lý chặt chẽ các thiết bị lưu trữ dữ liệu, nghiêm cấm việc di chuyển, thay đổi vị trí khi chưa được phép của người có thẩm quyền.

6. Quản lý và phân quyền truy cập phần mềm ứng dụng và cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ của người sử dụng. Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của nhân viên và phải được phê duyệt từ cấp trên.

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.

8. Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ, phương tiện lưu trữ.

Điều 13. Quản lý an toàn thiết bị đầu cuối

Các thiết bị đầu cuối khi kết nối vào hệ thống phải được quản lý như sau:

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

2. Các thiết bị đầu cuối phải được quản lý khi kết nối vào hệ thống mạng theo địa chỉ MAC, IP.

3. 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.

4. 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.

5. Cấu hình tối ưu và tăng cường bảo mật cho máy tính người sử dụng và thực hiện quy trình trước khi đưa vào hệ thống sử dụng:

a) Máy tính người dùng trước khi đưa vào sử dụng phải được đánh giá, rà soát các điểm yếu ATTT, bảo đảm sử dụng hệ điều hành có bản quyền, còn trong hạn được hỗ trợ cập nhật của hãng phát hành. Trong trường hợp có thông báo hết hỗ trợ cập nhật bản vá từ hãng, phải có kế hoạch nâng cấp, thay thế. Cập nhật bản vá hệ điều hành đầy đủ tại thời điểm đưa vào sử dụng và trong quá trình sử dụng.

b) Gỡ bỏ các phần mềm không cần thiết, cài đặt chương trình diệt virus. Không cấp tài khoản quản trị máy tính cho người dùng, không để người dùng tự ý cài đặt các phần mềm độc hại trên máy tính.

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

Điều 14. Quản lý phòng chống phần mềm độc hại

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

2. Hệ điều hành, phần mềm cài đặt trên máy chủ, máy trạm phải được cập nhật vá lỗ hổng bảo mật thường xuyên, kịp thời.

3. Cán bộ, công chức, viên chức và người lao động không được tự ý gỡ bỏ các phần mềm phòng, chống phần mềm độc hại trên máy tính khi chưa có sự đồng ý của người có thẩm quyền trong cơ quan.

4. Tất cả các máy tính của đơn vị phải được cấu hình vô hiệu hóa tính năng tự động thực thi (autoplay) các tập tin trên các thiết bị lưu trữ di động.

5. Các máy tính xách tay, thiết bị di động (điện thoại thông minh, máy tính bảng,...) trước khi kết nối vào mạng LAN nội bộ của cơ quan, đơn vị phải bảo đảm đã được cài chương trình phòng chống phần mềm độc hại và đã được kiểm duyệt về các phần mềm độc hại.

6. Tất cả các tập tin, thư mục phải được quét phần mềm độc hại trước khi sao chép, sử dụng.

7. Máy chủ chỉ được dùng để cài đặt các phần mềm, dịch vụ dùng chung của cơ quan, đơn vị; không cài đặt phần mềm không rõ nguồn gốc, phần mềm phục vụ mục đích cá nhân và mục đích khác, không phục vụ công việc.

8. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy trạm như: máy hoạt động chậm bất thường, cảnh bao từ phân mềm phòng chống phần mềm độc hại, tình trạng này lặp đi lặp lại nhiều lần, ở các vị trí khác nhau; quan trọng nhất là có dấu hiệu mất dữ liệu..., người sử dụng phải tắt máy, ngắt kết nối từ máy tính đến mạng LAN nội bộ, mạng WAN nội tỉnh, mạng Internet,... và báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý.

Điều 15. Quản lý giám sát an toàn hệ thống thông tin

Công tác triển khai: Hệ thống giám sát trung tâm; thông tin giám sát và danh mục các đối tượng giám sát; thực thi nhiệm vụ giám sát; nâng cao năng lực hoạt động giám sát; trách nhiệm giám sát an toàn thông tin của các Hệ thống thông tin của tỉnh được thực hiện theo 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.

Điều 16. Quản lý điểm yếu an toàn thông tin

1. Đơn vị vận hành hệ thống thông tin có trách nhiệm:

a) 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.

b) Quản trị viên hệ thống báo cáo lãnh đạo, cán bộ 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.

c) 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.

d) 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.

2. Đối với hệ thống, hệ thống thành phần được đề xuất cấp độ phải thực hiện 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.

3. Định kỳ hàng 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 thông tin khi có thông tin hoặc nhận được cảnh báo.

4. Hoạt động đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thực hiện theo quy định tại điểm c khoản 2 Điều 20 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.

Điều 17. Quản lý sự cố an toàn thông tin

Các hoạt động, quy trình, kế hoạch ứng cứu sự cố an toàn thông tin mạng cho các hệ thống thông tin của tỉnh thực hiện theo theo Quyết định số 390/QĐ-UBND ngày 11/4/2024 của Chủ tịch UBND tỉnh về việc ban hành Kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Bắc Ninh.

Điều 18. Quản lý an toàn người sử dụng đầu cuối

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

a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ phải tuân thủ các quy định của pháp luật về bảo đảm ATTT 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.

2. Cài đặt và sử dụng máy tính an toàn

a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về ATTT mạng. Chịu trách nhiệm bảo đảm ATTT 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 ATTT 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, xử lý.

d) Tham gia các chương trình đào tạo, hội nghị về ATTT mạng được cơ quan chức năng, đơn vị chuyên môn tổ chức.

Điều 19. Quản lý rủi ro an toàn thông tin

1. Xác định mức rủi ro

Mức ảnh hưởng	Tính bảo mật (C)	Tính toàn vẹn (I)	Tính sẵn sàng (A)
Đặc biệt nghiêm trọng (5)	Việc bị lộ thông tin trái phép làm ảnh hưởng đặc biệt nghiêm trọng đến quốc phòng, an ninh	Việc sửa đổi hoặc phá hủy trái phép thông tin làm ảnh hưởng đặc biệt nghiêm trọng đến quốc phòng, an ninh	Việc gián đoạn truy cập hoặc sử dụng thông tin/hệ thống thông tin làm ảnh hưởng đặc biệt nghiêm trọng đến quốc phòng, an ninh

Mức ảnh hưởng	Tính bảo mật (C)	Tính toàn vẹn (I)	Tính sẵn sàng (A)
Nghiêm trọng (4)	Việc bị lộ thông tin trái phép làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới quốc phòng, an ninh quốc gia	Việc sửa đổi hoặc phá hủy trái phép thông tin làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới quốc phòng, an ninh quốc gia	Việc gián đoạn truy cập hoặc sử dụng thông tin/hệ thống thông tin làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới quốc phòng, an ninh quốc gia
Vừa phải (3)	Việc bị lộ thông tin trái phép làm tổn hại nghiêm trọng tới sản xuất, lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại tới quốc phòng, an ninh quốc gia	Việc sửa đổi hoặc phá hủy trái phép thông tin làm tổn hại nghiêm trọng tới sản xuất, lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại tới quốc phòng, an ninh quốc gia	Việc gián đoạn truy cập hoặc sử dụng thông tin/hệ thống thông tin làm tổn hại nghiêm trọng tới sản xuất, lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại tới quốc phòng, an ninh quốc gia
Nhỏ (2)	Việc bị lộ thông tin trái phép làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng	Việc sửa đổi hoặc phá hủy trái phép thông tin làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng	Việc gián đoạn truy cập hoặc sử dụng thông tin/hệ thống thông tin làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng
Không đáng kể (1)	Việc bị lộ thông tin trái phép làm tổn hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân	Việc sửa đổi hoặc phá hủy trái phép thông tin làm tổn hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân	Việc gián đoạn truy cập hoặc sử dụng thông tin/hệ thống thông tin làm tổn hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân

2. Quy trình đánh giá và quản lý rủi ro

(Quy trình đánh giá và quản lý rủi ro của hệ thống thông tin thực hiện theo hướng dẫn tại Phụ lục kèm theo).

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.

3. Việc thực hiện kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin được thực hiện theo quy định của pháp luật hiện hành.

Chương IV
TỔ CHỨC BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 21. Trách nhiệm của tổ chức, cá nhân bên ngoài khi tham gia sử dụng hệ thống thông tin của cơ quan nhà nước, để giao tiếp, cung cấp và trao đổi thông tin số với cơ quan nhà nước

1. Nghiêm chỉnh thi hành quy chế này và các quy định khác của pháp luật về bảo đảm ATTT mạng.

2. Khi phát hiện sự cố ảnh hưởng đến an toàn hệ thống thông tin, phải thông báo ngay với cơ quan nhà nước, nơi tổ chức, cá nhân đang thực hiện giao tiếp.

3. Các tổ chức, cá nhân tham gia vào quá trình ứng dụng CNTT trên địa bàn tỉnh, chịu sự thanh tra, kiểm tra của các cơ quan nhà nước có thẩm quyền về lĩnh vực ATTT.

Điều 22. Trách nhiệm của các cơ quan, đơn vị

1. Bảo đảm an toàn thông tin mạng theo quy định hiện hành của các cấp có thẩm quyền, quy chế này và các quy chế nội bộ khác.

2. Báo cáo định kỳ vào ngày 15/10 hàng năm hoặc đột xuất theo yêu cầu về Sở Thông tin và Truyền thông để tổng hợp, báo cáo Ủy ban nhân dân tỉnh, Bộ Thông tin và Truyền thông.

3. Tuân thủ và bảo đảm ATTT trong ứng dụng CNTT, bảo đảm an toàn thông tin mạng nội bộ của cơ quan, đơn vị theo hướng dẫn của Sở Thông tin và Truyền thông theo quy định của quy chế này và các quy định khác của pháp luật có liên quan.

4. Tuyên truyền, phổ biến quy chế này và các quy định khác của pháp luật có liên quan về ATTT trong phạm vi trách nhiệm và quyền hạn của từng cơ quan.

5. Xác định và trình cấp có thẩm quyền phê duyệt cấp độ hệ thống thông tin của cơ quan, đơn vị.

6. Khi được kiểm tra công tác bảo đảm an toàn thông tin mạng tại cơ quan, đơn vị cử cán bộ có chuyên môn về CNTT tham gia đoàn kiểm tra; phối hợp với đoàn kiểm tra xây dựng các tiêu chí và quy trình kỹ thuật kiểm tra công tác bảo đảm ATTT.

7. Các sở, ban, ngành, UBND các huyện, thị xã, thành phố hàng năm, căn cứ khả năng cân đối ngân sách, tiêu chuẩn định mức khi được cấp có thẩm quyền giao nhiệm vụ bảo đảm ATTT mạng, các cơ quan, đơn vị phối hợp với Sở Tài chính rà soát (đối với nguồn kinh phí thường xuyên) để trình cấp có thẩm quyền bố trí kinh phí theo quy định hiện hành, phối hợp với Sở Kế hoạch và Đầu tư (đối

với nguồn kinh phí đầu tư công) triển khai thực hiện các dự án, nhiệm vụ bảo đảm ATTT theo quy định.

Điều 23. Trách nhiệm của cán bộ, công chức, viên chức, người lao động trong cơ quan nhà nước.

1. Nghiêm chỉnh thi hành quy chế này và các quy định khác của pháp luật về bảo đảm ATTT.

2. Khi phát hiện sự cố ảnh hưởng đến an toàn hệ thống thông tin, phải thông báo ngay đến cán bộ, công chức chuyên trách CNTT của đơn vị.

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

4. Cán bộ, công chức, viên chức chuyên trách CNTT:

a) Theo nhiệm vụ được Thủ trưởng cơ quan, đơn vị phân công, chịu trách nhiệm tham mưu chuyên môn và vận hành bảo đảm an toàn hệ thống thông tin tại cơ quan, đơn vị;

b) Hướng dẫn, hỗ trợ người dùng tại cơ quan, đơn vị giải pháp phòng, chống vi rút, mã độc máy tính. Thực hiện việc đánh giá, báo cáo các rủi ro và mức độ các rủi ro ảnh hưởng đến hoạt động hệ thống thông tin của đơn vị, các giải pháp cơ bản khắc phục các rủi ro:

c) Phối hợp với các cá nhân, tổ chức có liên quan trong việc kiểm tra, phát hiện, phòng ngừa, đấu tranh, ngăn chặn xâm phạm ATTT; tham gia khắc phục các sự cố mất ATTT.

Điều 24. Trách nhiệm của Sở Thông tin và Truyền thông

1. Tham mưu UBND tỉnh về công tác bảo đảm ATTT trên địa bàn tỉnh và chịu trách nhiệm trước UBND tỉnh trong việc bảo đảm an toàn cho các hệ thống thông tin cấp tỉnh.

2. Xây dựng và triển khai các Kế hoạch, chương trình, đào tạo về ATTT trong ứng dụng CNTT trên địa bàn tỉnh.

3. Tùy theo mức độ sự cố, phối hợp Trung tâm ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC) và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố ATTT trên địa bàn tỉnh; cảnh báo các vấn đề về ATTT trong các cơ quan nhà nước trên địa bàn tỉnh.

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

5. Hướng dẫn, hỗ trợ sao lưu dự phòng các thông tin, cơ sở dữ liệu của các cơ quan nhà nước một cách an toàn.

6. Hướng dẫn, giám sát các đơn vị xây dựng quy chế và thực hiện việc bảo đảm an toàn cho hệ thống thông tin theo quy định; hướng dẫn các cơ quan về khung báo cáo; định kỳ tổng hợp báo cáo Ủy ban nhân dân tỉnh và Bộ Thông tin và Truyền thông và các cơ quan có thẩm quyền về công tác ATTT số trên địa bàn tỉnh.

7. Tuyên truyền và định hướng tuyên truyền, phối hợp tuyên truyền đến các phương tiện truyền thông đại chúng trên địa bàn tỉnh về công tác bảo đảm ATTT.

8. Hàng năm, tổ chức đào tạo hoặc cử nhân sự tham gia các khoá đào tạo chuyên sâu về ATTT mạng cho cán bộ, công chức chuyên trách CNTT bảo đảm ATTT mạng của các cơ quan, đơn vị.

9. Tham mưu xây dựng kế hoạch hàng năm, phối hợp với Công an tỉnh và các đơn vị có liên quan tổ chức kiểm tra định kỳ bảo đảm an toàn thông tin mạng, hệ thống thông tin theo cấp độ của các cơ quan, đơn vị.

10. Tổ chức đánh giá an toàn thông tin mạng cho các hệ thống thông tin dùng chung, hạ tầng Trung tâm tích hợp dữ liệu của tỉnh hàng năm theo quy định.

11. Tổng hợp Báo cáo định kỳ của các cơ quan đơn vị (vào ngày 15/10 hàng năm) báo cáo Ủy ban nhân dân tỉnh, Bộ Thông tin và Truyền thông theo quy định.

12. Thông báo cho các đầu mối quản trị công nghệ thông tin tại các cơ quan, đơn vị thời gian cụ thể khi có cập nhật thay đổi hệ thống hoặc báo ngay cho các đầu mối khi có sự cố của các hệ thống dùng chung để các đơn vị chủ động thông báo cho đơn vị.

Điều 25. Trách nhiệm của Sở Tài chính, Sở Kế hoạch và Đầu tư

Hàng năm, căn cứ khả năng cân đối ngân sách, tiêu chuẩn định mức khi được cấp có thẩm quyền giao nhiệm vụ bảo đảm ATTT mạng: Sở Tài chính phối hợp với các cơ quan, đơn vị rà soát nguồn kinh phí thường xuyên để trình cấp có thẩm quyền bố trí kinh phí theo quy định hiện hành; Sở Kế hoạch và Đầu tư rà soát nguồn kinh phí đầu tư công triển khai thực hiện các dự án, nhiệm vụ bảo đảm ATTT theo quy định.

Điều 26. Trách nhiệm của Trung tâm Công nghệ thông tin và Truyền thông – Sở Thông tin và Truyền thông

1. Trung tâm Công nghệ thông tin và Truyền thông chịu trách nhiệm quản trị, vận hành và bảo đảm an toàn thông tin cho các hệ thống dùng chung của tỉnh căn cứ theo Quyết định số 15/2023/QĐ-UBND ngày 18/8/2023 của UBND tỉnh về việc ban hành Quy chế quản lý, vận hành và sử dụng Trung tâm Dữ liệu tỉnh Bắc Ninh và các quy định tại Quy chế này.

2. Khảo sát, triển khai, xây dựng mô hình kết nối mạng nội bộ (LAN) bảo đảm an toàn thông tin chung cho các cơ quan, đơn vị triển khai thực hiện.

Điều 27. Trách nhiệm của các doanh nghiệp cung cấp dịch vụ viễn thông, CNTT và Internet

1. Đầu tư xây dựng, trang bị hạ tầng kỹ thuật đáp ứng đầy đủ các yêu cầu, tiêu chuẩn kỹ thuật theo quy định của Bộ Thông tin và Truyền thông về ATTT và các nội dung quy định tại Quy chế này.

2. Phối hợp với Sở Thông tin và Truyền thông để tham gia các hoạt động điều phối, ứng cứu, khắc phục sự cố thông tin bảo đảm ATTT mạng cho các cơ quan, đơn vị trong quá trình sử dụng, khai thác sử dụng dịch vụ.

3. Bảo đảm mạng truyền số liệu chuyên dùng cung cấp cho các cơ quan, đơn vị được thông suốt, ổn định.

4. Chịu hoàn toàn trách nhiệm nếu có sự cố xảy ra mà thời gian xử lý vượt quá 4 giờ kể từ thời điểm nhận được thông tin sự cố và chịu trách nhiệm trước

Ủy ban nhân dân tỉnh về chất lượng dịch vụ nếu để số sự cố xảy ra quá 3 lần/tháng/01 đơn vị.

Chương V
ĐIỀU KHOẢN THI HÀNH

Điều 28. Tổ chức thực hiện

1. Sở Thông tin và Truyền thông chủ trì, phối hợp với các sở, ban, ngành, UBND các huyện, thị xã, thành phố và các tổ chức, cá nhân có liên quan triển khai thực hiện Quy chế này.

2. Thủ trưởng các sở, ban, ngành, đơn vị thuộc UBND tỉnh, Chủ tịch UBND các huyện, thị xã, thành phố và thủ trưởng các cơ quan, đơn vị liên quan chịu trách nhiệm tổ chức triển khai thực hiện Quy chế tại cơ quan, đơn vị, địa phương mình.

Điều 29. Sửa đổi, bổ sung Quy chế

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

Phụ lục

QUY TRÌNH ĐÁNH GIÁ VÀ QUẢN LÝ RỦI RO

(Kèm theo Quyết định số 41/2024/QĐ-UBND ngày 05/9/2024 của UBND tỉnh)

1. Bước thiết lập bối cảnh, cơ quan, tổ chức cần đưa ra thông tin tổng quan, mục tiêu, quy mô, phạm vi và các thành phần của hệ thống cần bảo vệ.

Bước này, cơ quan, tổ chức cần đưa ra thông tin tổng quan, mục tiêu, quy mô, phạm vi và các thành phần của hệ thống cần bảo vệ, bao gồm nhưng không giới hạn các thông tin sau:

a) Thông tin Chủ quản hệ thống thông tin;

b) Thông tin Đơn vị vận hành;

c) Chức năng, nhiệm vụ, cơ cấu tổ chức của đơn vị vận hành;

d) Các cơ quan, tổ chức liên quan;

e) Phạm vi, quy mô của hệ thống.

2. Bước đánh giá rủi ro, cơ quan, tổ chức cần thực hiện nhận biết rủi ro, phân tích rủi ro và ước lượng rủi ro. Kết quả của việc thực hiện nội dung này là cần xác định tài sản, điểm yếu, mối đe dọa, hậu quả và mức ảnh hưởng đối với cơ quan, tổ chức khi rủi ro xảy ra đối với tài sản.

a) Tiêu chí chấp nhận rủi ro: Việc xử lý toàn bộ rủi ro được xác định là khó khả thi với bất kỳ cơ quan, tổ chức nào. Do đó, các rủi ro có thể xem xét giảm thiểu đến mức chấp nhận được; tiêu chí chấp nhận rủi ro phụ thuộc vào các chính sách, mục đích, mục tiêu bảo đảm an toàn thông tin của cơ quan, tổ chức và các lợi ích của các bên liên quan; mỗi tổ chức cần phải xác định mức chấp nhận rủi ro của riêng tổ chức mình. Việc xác định các tiêu chí chấp nhận rủi ro cần xem xét đến các yếu tố như: Nguồn lực để xử lý rủi ro so với hiệu quả mang lại sau khi rủi ro được xử lý, khả năng xử lý rủi ro theo điều kiện thực tế của cơ quan, tổ chức của mình.

b) Tiêu chí chấp nhận rủi ro có thể bao gồm nhiều ngưỡng với các tiêu chí tương ứng, căn cứ theo mục tiêu bảo đảm an toàn thông tin mà tổ chức đưa ra, như sau:

- Hệ thống thông tin cấp độ 3, có xử lý thông tin bí mật nhà nước, chỉ chấp nhận tồn tại các rủi ro ở mức thấp. Chỉ chấp nhận tồn tại các rủi ro mức trung bình đối với hệ thống thông tin cấp độ 3, không xử lý thông tin bí mật nhà nước;

- Hệ thống thông tin cấp độ 1 hoặc cấp độ 2, chỉ chấp nhận tồn tại các rủi ro mức trung bình.

- Cơ quan, tổ chức cần xác định rõ phạm vi thực hiện đánh giá và quản lý rủi ro để bảo toàn tài sản được bảo vệ trong quy trình thực hiện. Để xác định phạm vi, giới hạn, cơ quan, tổ chức cần xác định rõ thông tin liên quan sau:

- Phạm vi quản lý an toàn thông tin: Các mục tiêu bảo đảm an toàn thông tin của cơ quan, tổ chức; các quy định pháp lý phải tuân thủ; quy chế, chính sách bảo đảm an toàn thông tin của tổ chức.

- Phạm vi kỹ thuật: Sơ đồ tổng thể (vật lý, logic) và các thành phần trong hệ thống (thiết bị mạng, bảo mật, máy chủ, thiết bị đầu cuối…); xác định các hệ thống thông tin khác có liên quan hoặc có kết nối đến hoặc có ảnh hưởng quan trọng tới hoạt động bình thường của hệ thống thông tin được đề xuất; trong đó,

xác định rõ mức độ ảnh hưởng đến hệ thống thông tin đang được đề xuất cấp độ khi các hệ thống này bị mất an toàn thông tin; danh mục các nguy cơ tấn công mạng, mất an toàn thông tin đối với hệ thống và các ảnh hưởng.

- Cơ quan, tổ chức cần xây dựng phương án, kế hoạch thực hiện quản lý rủi ro an toàn thông tin. Nội dung phương án, kế hoạch, trách nhiệm của các đơn vị, bộ phận liên quan cần đưa vào quy chế bảo đảm an toàn thông tin của cơ quan, tổ chức để thực hiện. Dưới đây là một số nội dung cơ bản cần thực hiện để tổ chức thực hiện quản lý rủi ro an toàn thông tin:

+ Phương án, kế hoạch thực hiện đánh giá và quản lý rủi ro;

+ Quy trình tổ chức thực hiện đánh giá và quản lý rủi ro;

+ Cơ chế phối hợp với các bên liên quan trong quá trình thực hiện;

+ Phương án, kế hoạch giám sát quy trình đánh giá và quản lý rủi ro.

- Nhận biết rủi ro là các bước để xác định ra các rủi ro, hậu quả và mức thiệt hại tương ứng. Để xác định được rủi ro, cơ quan, tổ chức cần thực hiện các bước sau:

+ Nhận biết về tài sản để xác định danh mục các tài sản của cơ quan, tổ chức cần bảo vệ bao gồm thông tin, hệ thống thông tin.

+ Nhận biết về mối đe dọa để xác định các mối đe dọa đối với mỗi tài sản.+ Nhận biết về điểm yếu để xác định các điểm yếu có thể tồn tại đối với mỗi tài sản.

+ Kết quả của bước nhận biết rủi ro là danh mục các mối đe dọa và điểm yếu đối với các tài sản được xác định.

- Phân tích rủi ro để xác định ra các mức ảnh hưởng, các hậu quả đối với cơ quan, tổ chức trên cơ sở thực hiện bước nhận biết rủi ro ở trên. Để phân tích rủi ro, cơ quan, tổ chức cần thực hiện các bước sau:

+ Đánh giá các hậu quả để xác định mức ảnh hưởng đối với cơ quan, tổ chức khi tài sản bị khai thác điểm yếu gây ra các mối đe doạ.

+ Đánh giá khả năng xảy ra đối với từng loại sự cố.

+ Kết quả của bước phân tích rủi ro là xác định được các hậu quả, mức ảnh hưởng mà cơ quan, tổ chức phải xử lý.

- Ước lượng rủi ro để xác định ra các rủi ro và mức rủi ro tương ứng mà cơ quan, tổ chức phải xử lý. Mức rủi ro được xác định dựa vào 03 tham số được xác định ở bước trên.

3. Bước xử lý rủi ro, cơ quan, tổ chức cần xác định các phương án xử lý rủi ro, bao gồm các biện pháp quản lý và kỹ thuật để có thể xử lý, giảm thiểu các mối đe dọa có thể xảy ra đối với tài sản, dẫn tới hậu quả cho cơ quan, tổ chức.

Cơ quan, tổ chức có thể lựa chọn các phương án xử lý rủi ro khác nhau để bảo đảm đạt được các mục tiêu bảo đảm an toàn thông tin của đơn vị mình. Xử lý rủi ro có thể được thực hiện bởi một hoặc kết hợp nhiều phương án sau: thay đổi rủi ro, duy trì rủi ro, tránh rủi ro và chia sẻ rủi ro, cụ thể như dưới đây:

- Thay đổi rủi ro:

+ Thay đổi rủi ro là phương án thực hiện các biện pháp xử lý, khắc phục nhằm giảm mức rủi ro đã được xác định sao cho các rủi ro tồn đọng được đánh giá lại ở mức chấp nhận được;

+ Để thực hiện phương án này, cơ quan, tổ chức cần xây dựng một hệ thống các biện pháp kiểm soát phù hợp. Các biện pháp được lựa chọn căn cứ vào các

tiêu chí liên quan đến chi phí, đầu tư và thời gian triển khai, trên cơ sở cân đối giữa nguồn lực bỏ ra và lợi ích đem lại đối với tổ chức khi thực hiện xử lý rủi ro đó.

- Duy trì rủi ro: Duy trì rủi ro là phương án chấp nhận rủi ro đã xác định mà không đưa ra các phương án xử lý để giảm thiểu rủi ro. Việc xác định rủi ro nào có thể được chấp nhận dựa vào mức rủi ro và tiêu chí chấp nhận rủi ro.

- Tránh rủi ro: Tránh rủi ro là phương án xử lý khi cơ quan, tổ chức phải đối mặt với mức rủi ro quá cao bằng cách làm thay đổi, loại bỏ hoặc dừng hoạt động của hệ thống, quy trình nghiệp vụ hoặc hoạt động của cơ quan, tổ chức để không phải đối mặt với rủi ro đã xác định. Tránh rủi ro là phương án thích hợp khi rủi ro được xác định vượt quá khả năng chấp nhận rủi ro của tổ chức.

- Chia sẻ rủi ro: Chia sẻ rủi ro là phương án chuyển rủi ro, một phần rủi ro phải đối mặt cho cơ quan, tổ chức khác. Phương án chia sẻ rủi ro thường được thực hiện khi cơ quan, tổ chức xác định rằng việc giải quyết rủi ro yêu cầu chuyên môn hoặc nguồn lực được cung cấp tốt hơn bởi các tổ chức khác.

- Chấp nhận rủi ro: Chấp nhận rủi ro là việc xem xét, đánh giá các rủi ro tồn đọng, chưa được xử lý hoàn toàn để đánh giá lại mức rủi ro sau xử lý có thể được chấp nhận hay không. Bởi vì có thể hệ thống tồn tại những rủi ro không có phương án xử lý triệt để mà chỉ có thể giảm thiểu.

4. Quá trình truyền thông và tư vấn rủi ro là quá trình cơ quan, tổ chức cần trao đổi, tham vấn ý kiến của các bên liên quan để có thông tin đầu vào khi thực hiện các bước ở trên; thực hiện tuyên truyền, phổ biến các nguy cơ, rủi ro có thể xảy ra.

Truyền thông và tư vấn rủi ro an toàn thông tin là hoạt động nhằm đào tạo, tuyên truyền nâng cao nhận thức cho các bên liên quan đến hoạt động đánh giá và quản lý rủi ro. Bên cạnh đó, việc này cũng nhằm đạt được sự thống nhất giữa các bên liên quan. Ví dụ trong trường hợp lựa chọn phương án chia sẻ rủi ro.

Cơ quan, tổ chức cần xây dựng kế hoạch truyền thông rủi ro định kỳ hoặc đột xuất. Hoạt động truyền thông rủi ro phải được thực hiện liên tục và thường xuyên.

5. Quá trình giám sát và soát xét rủi ro, cơ quan, tổ chức giám sát và đánh giá tuân thủ, tính hiệu quả của việc thực hiện việc quản lý rủi ro.

- Giám sát và soát xét rủi ro an toàn thông tin nhằm bảo đảm hoạt động đánh giá và quản lý rủi ro an toàn thông tin được thực hiện thường xuyên liên tục theo quy chế, chính sách bảo đảm an toàn thông tin của cơ quan, tổ chức và được cấp có thẩm quyền phê duyệt.

- Giám sát và soát xét các yếu tố rủi ro, việc giám sát và soát xét các yếu tố rủi ro cần bảo đảm các yếu tố sau:

+ Quản lý được các tài sản mới, sự thay đổi của tài sản, giá trị của tài sản;

+ Sự thay đổi, xuất hiện mới các mối đe dọa;

+ Sự thay đổi, xuất hiện mới các điểm yếu;

+ Sự thay đổi, xuất hiện mới các rủi ro;

+ Kết quả của việc giám sát và soát xét các yếu tố rủi ro là việc cập nhật thường xuyên, liên tục sự thay đổi đối với các yếu tố rủi ro được đề cập ở trên.

- Giám sát soát xét và cải tiến quản lý rủi ro:

+ Để bảo đảm hoạt động quản lý rủi ro an toàn thông tin được mang lại hiệu quả, việc giám sát, soát xét và cải tiến quy trình quản lý rủi ro an toàn thông tin cần được thực hiện thường xuyên, liên tục.

+ Các tiêu chí được sử dụng để giám sát soát xét và cải tiến quản lý rủi ro có thể bao gồm, nhưng không giới hạn các yếu tố sau: Các yếu tố liên quan đến quy định pháp lý; phương pháp tiếp cận đánh giá rủi ro; các loại tài sản và giá trị tài sản; tiêu chí tác động; tiêu chí ước lượng rủi ro; tiêu chí chấp nhận rủi ro; các nguồn lực cần thiết.