Ký bởi: Ủy ban nhân dân xã Chà Tở

ỦY BAN NHÂN DÂN **XÃ CHÀ TỞ**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 398 /QĐ-UBND	*Chà Tở, ngày 30 tháng 12 năm 2025*

QUYẾT ĐỊNH

Ban hành Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của các cơ quan nhà nước trên địa bàn xã Chà Tở

ỦY BAN NHÂN DÂN XÃ CHÀ TỞ

Căn cứ Luật Tổ chức chính quyền địa phương số 72/2025/QH15 ngày 16/6/2025;

Căn cứ Luật Công nghệ thông tin ngày 15 tháng 8 năm 2025;

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 72/2013/NĐ-CP ngày 15 tháng 7 năm 2013 của Chính phủ về 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 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 về 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;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của 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 Thông tư số 27/2017/TT-BTTTT ngày 20 tháng 10 năm 2017 của Bộ Thông tin và Truyền thông quy định về việc quản lý vận hành, sử dụng và bảo đảm an toàn thông tin trên Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;

Căn cứ Quyết định số 19/2022/QĐ-UBND ngày 27/6/2022 của Ủy ban nhân dân tỉnh Điện Biên về việc Ban hành quy chế đảm bảo an toàn thông tin mạng trọng hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của cơ quan, đơn vị tỉnh Điện Biên;

Theo đề nghị của Phòng Văn hóa - Xã hội.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của các cơ quan nhà nước trên địa bàn xã Chà Tở".

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

Điều 3. Chánh Văn phòng HĐND và UBND xã Chà Tở, Thủ trưởng các cơ quan, phòng, thuộc xã Chà Tở và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Ủy ban nhân dân tỉnh (b/c);
- Công an tỉnh (b/c);
- Sở Khoa học và Công nghệ (b/c);
- Thường trực Đảng ủy;
- Thường trực HĐND xã;
- Lãnh đạo UBND xã;
- Ủy ban MTTQ Việt Nam xã;
- Công an xã;
- Các cơ quan, đơn vị thuộc UBND xã;
- Lưu: VT, VHXH.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

U.B.N.D XÃ CHÀ TỞ T.ĐIỆN BIÊN

Lò Văn Nọi

ỦY BAN NHÂN DÂN XÃ CHÀ TỞ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY CHẾ

Ban hành Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của các cơ quan nhà nước trên địa bàn xã Chà Tở

(Ban hành kèm theo Quyết định số /QĐ-UBND ngày tháng 12 năm 2025 của UBND xã Chà Tở)

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 các hệ thống thông tin tại UBND xã Chà Tở.

2. Đối tượng áp dụng:

a) Các cơ quan, phòng, ban thuộc xã; các đơn vị sự nghiệp công lập trực thuộc Ủy ban nhân dân xã; Các cơ quan Đảng, đoàn thể, 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 trên địa bàn xã (sau đây gọi tắt là các cơ quan, đơn vị).

b) Cán bộ, công chức, viên chức, người lao động (gọi tắt là CB, CC, VC, NLĐ) và các tổ chức, cá nhân có liên quan tham gia vận hành, khai thác các hệ thống thông tin tại các cơ quan, đơn vị.

c) Khuyến khích các cơ quan, đơn vị khác trên địa bàn xã áp dụng quy chế này trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số tại cơ quan, đơn vị.

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

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

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

4. *Hệ thống thông tin quan trọng quốc gia* là hệ thống thông tin mà khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới quốc phòng, an ninh quốc gia.

5. *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.

6. *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.

7. *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.

8. *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.

9. *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.

10. *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.

11. *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.

12. *Hệ thống lọc phần mềm độc hại* là tập hợp phần cứng, phần mềm được kết nối vào mạng để phát hiện, ngăn chặn, lọc và thống kê phần mềm độc hại.

13. *Địa chỉ điện tử* là địa chỉ được sử dụng để gửi, nhận thông tin trên mạng bao gồm địa chỉ thư điện tử, số điện thoại, địa chỉ Internet và hình thức tương tự khác.

14. *Xung đột thông tin* là việc hai hoặc nhiều tổ chức trong nước và nước ngoài sử dụng biện pháp công nghệ, kỹ thuật thông tin gây tổn hại đến thông tin, hệ thống thông tin trên mạng.

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

16. *Chủ thể thông tin cá nhân* là người được xác định từ thông tin cá nhân đó.

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

18. *Mật mã dân sự* là kỹ thuật mật mã và sản phẩm mật mã được sử dụng để bảo mật hoặc xác thực đối với thông tin không thuộc phạm vi bí mật nhà nước.

19. *Sản phẩm an toàn thông tin mạng* là phần cứng, phần mềm có chức năng bảo vệ thông tin, hệ thống thông tin.

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

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 thông tin.

2. Nguyên tắc

1. Hoạt động an toàn thông tin mạng của cơ quan, tổ chức, cá nhân phải đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước, giữ vững ổn định chính trị, trật tự, an toàn xã hội và thúc đẩy phát triển kinh tế - xã hội.

2. Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác.

3. Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức.

4. Hoạt động an toàn thông tin mạng phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.

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 ngày 19/11/2015. Cụ thể:

a) Ngăn chặn việc truyền tải thông tin trên mạng, can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật.

b) Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới khả năng truy nhập hệ thống thông tin của người sử dụng.

c) Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin mạng của hệ thống thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin.

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

đ) Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân.

e) Xâm nhập trái pháp luật bí mật mật mã và thông tin đã mã hóa hợp pháp của cơ quan, tổ chức, cá nhân; tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin về khách hàng sử dụng hợp pháp sản phẩm mật mã dân sự; sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc.

2. Tự ý lắp đặt các thiết bị phát sóng Wifi (Access Point, Router wifi, USB Wifi, Wifi mesh) vào mạng máy tính của cơ quan, đơn vị và lắp đặt các thiết bị tiếp sóng Wifi (Wireless card, wireless USB, Wifi Repeater) trên máy tính có kết nối mạng nội bộ để truy cập mạng wifi ngoài khi chưa được phê duyệt của Lãnh đạo cơ quan, đơn vị.

3. Lợi dụng mạng để truyền bá thông tin, quan điểm, thực hiện các hành vi gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, lợi ích quốc gia trên mạng; phá hại khối đại đoàn kết toàn dân; tuyên truyền chiến tranh xâm lược, khủng bố; gây hận thù, mâu thuẫn giữa các dân tộc, sắc tộc, tôn giáo và bài ngoại.

4. Lợi dụng mạng để truyền bá trái phép tài liệu, hình ảnh, âm thanh hoặc dạng thông tin khác nhằm kích động bạo lực, dâm ô, đồi trụy, tội ác, tệ nạn xã hội, mê tín dị đoan, phá hoại thuần phong, mỹ tục của dân tộc; bôi nhọ, gây thù hận, xâm hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân.

5. Tự ý tải về, chia sẻ dưới mọi hình thức các dữ liệu, tài liệu, số liệu nội bộ, những văn bản chưa được cấp có thẩm quyền công khai lên mạng internet và các phương tiện thông tin đại chúng khác.

Chương II
ĐẢM BẢO AN TOÀN THÔNG TIN TRONG TỔ CHỨC

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 xã Chà Tở giao Văn phòng HĐND và UBND là đơn vị đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin.

b) Văn phòng HĐND và UBND xã làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng tại các đơn vị.

c) Văn phòng HĐND và UBND xã chủ trì, phối hợp với các đơn vị có liên quan tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hàng năm hoặc theo chỉ đạo của tỉnh đối với các cơ quan nhà nước trong tỉnh.

2. Là 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 Công an tỉnh; Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Điện Biên Sở Khoa học Công nghệ hoặc Trung tâm Công nghệ và Nền tảng số và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin mạng. Liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin mạng.

Điều 6. Bảo đảm nguồn nhân lực

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

- Có bằng tốt nghiệp đại học chuyên ngành máy tính, CNTT hoặc ATTT.

- Đáp ứng được các quy định của Thông tư số 45/2017/TT-BTTTT của Bộ Thông tin và Truyền thông Quy định tiêu chuẩn chức danh nghề nghiệp viên chức chuyên ngành CNTT;

- Có ít nhất 2 năm kinh nghiệm;

- Có cam kết giữ bí mật thông tin liên quan đến công việc.

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

Công tác tuyển dụng thực hiện theo theo Nghị định 115/2020/NĐ-CP ngày 25/9/2020 của Chính phủ quy định về tuyển dụng, sử dụng và quản lý viên chức; Nghị định số 138/2020/NĐ-CP ngày 27/11/2022 của Chính phủ quy định về tuyển dụng, sử dụng và quản lý công chức và điều kiện tuyển dụng công chức, viên chức, người lao động về làm việc tại Bộ Nội vụ, theo đó trong quá trình tuyển dụng có thành lập Hội đồng tuyển dụng, bao gồm các chuyên gia có trình độ chuyên môn để kiểm tra, đánh giá ứng viên. Các chuyên gia cần đáp ứng các yêu cầu sau:

- Đã tốt nghiệp đại học các ngành nhân sự, quản trị nhân lực, ATTT hoặc các ngành có liên quan;

- Kinh nghiệm tối thiểu trong lĩnh vực tuyển dụng 2 năm;

- Có kiến thức và kinh nghiệm trong việc tìm kiếm nguồn nhân sự thông qua các kênh tuyển dụng, mạng xã hội hay các trang thông tin điện tử (trang web) tuyển dụng.

Điều 7. Quy định về việc thực hiện bảo đảm an toàn thông tin trong quá trình làm việc

1. Quy định về thực hiện nội quy, quy chế bảo đảm ATTT cho người sử dụng, công chức, viên chức, người lao động quản lý và vận hành hệ thống

a) Đối với người sử dụng:

- Có trách nhiệm tuân thủ các quy định, hướng dẫn bảo đảm ATTT và các quy định của pháp luật, đảm bảo ATTT đối với từng vị trí công việc. Máy tính, thiết bị mạng trước khi tham gia vào hệ thống phải được kiểm tra khả năng đáp ứng các yêu cầu về ATTT và được dán tem ATTT;

- 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 trước pháp luật về các hành vi làm lộ, lọt thông tin, nội

dung bí mật nhà nước do không tuân thủ, quy định của pháp luật, UBND xã Chà Tở;

- Đổi mật khẩu ngay sau khi được cấp tài khoản đăng nhập các dịch vụ, ứng dụng, phần mềm dùng chung của tỉnh. Giữ bí mật tài khoản cá nhân khi tham gia khai thác, không ghi mật khẩu ra những nơi người khác có thể biết; không lưu trữ, truyền, gửi mật khẩu khi chưa được mã hóa an toàn và chia sẻ mật khẩu của cá nhân cho người khác;

- 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) Với cán bộ quản lý và vận hành hệ thống

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

- Cán bộ phụ trách phải tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin.

- Thực hiện chặt chẽ việc kiểm soát thay đổi của hệ thống thông tin: Phiên bản phần mềm, cấu hình phần cứng, tài liệu, quy trình vận hành; ghi đầy đủ thông tin mạng trong các bản ghi nhật ký hệ thống và lưu trữ nhật ký tối thiểu 06 tháng để phục vụ việc quản lý, kiểm soát thông tin mạng.

2. Định kỳ hàng năm người sử dụng được tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin theo chương trình, nội dung tại Kế hoạch số 1936/KH-UBND ngày 24/6/2022 về tuyên truyền, nâng cao nhận thức và phổ biến kiến thức về an toàn thông tin đến năm 2025 trên địa bàn tỉnh Điện Biên.

3. Định kỳ hàng năm người sử dụng được tổ chức đào tạo các kỹ năng cơ bản về an toàn thông tin theo chương trình, nội dung tại Kế hoạch số 1064/KH-UBND ngày 14/4/2021 của UBND tỉnh Điện Biên về Đào tạo và phát triển nguồn nhân lực an toàn thông tin trong cơ quan nhà nước tỉnh Điện Biên giai đoạn 2021-2025 trên địa bàn tỉnh.

Điều 8. Quy định đối với công chức, viên chức, người lao động nghỉ việc hoặc thay đổi công việc

1. 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.

2. 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:

a) 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.

b) 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.

c) Vô hiệu hóa tất cả các quyền ra vào trung tâm dữ liệu của công chức, viên chức, người lao động thôi việc tại các trụ sở làm việc của đơn vị quản lý.

d) 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.

đ) 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 đảm bảo đã hoàn toàn được gỡ bỏ khỏi hệ thống.

3. 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 III
BẢO ĐẢM AN TOÀN THÔNG TIN TRONG THIẾT KẾ, XÂY DỰNG HỆ THỐNG THÔNG TIN

Điều 9. Thiết kế, xây dựng hệ thống thông tin

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

- Tài liệu phân tích lựa chọn kiến trúc, công nghệ;

- Tài liệu thiết kế tổng thể hệ thống thể hiện thiết kế hạ tầng và kết nối các thành phần của hệ thống;

- 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 (nếu có);

- 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. Đơn vị thiết kế, xây dựng hệ thống thông tin phải cung cấp các tài liệu "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 miêu tả hệ thống dưới nhiều góc nhìn khác nhau, bao gồm:

- Thiết kế kiến trúc ứng dụng;

- Thiết kế kiến trúc dữ liệu;

- Thiết kế kiến trúc vật lý.

3. Đơn vị thiết kế, xây dựng hệ thống thông tin phải cung cấp tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ 3 trở lên được quy định tại Thông tư số 12/2022/TT-BTTTT.

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

- Đảm bảo có từ 2 - 3 công nghệ được phân tích và đưa ra phương án lựa chọn;

- 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 thiết kế, xây dựng hệ thống thông tin, 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 đặt ra đối với hệ thống, xây dựng kế hoạch trước khi có thay đổi, kèm theo các tài liệu sau:

- Căn cứ thực hiện thay đổi (công văn, tờ trình);

- Kế hoạch chi tiết các bước thực hiện.

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

- Hồ sơ thiết kế được giữ gìn bí mật, bảo quản theo chế độ tài liệu mật, không được mang hồ sơ thiết kế ra khỏi cơ quan hoặc tùy tiện cung cấp hồ sơ thiết kế cho cá nhân, đơn vị khác.

- Hồ sơ thiết kế phải được cất vào tủ có khóa. Những đợt nghỉ lễ, tết dài ngày phải niêm phong tủ đựng văn bản, tài liệu và phòng làm việc.

- Hồ sơ thiết kế được sắp xếp một cách khoa học để dễ quản lý, dễ nộp lưu và dễ tìm khi cần. Phải có những cặp khác nhau để đựng những loại hồ sơ, văn bản, tài liệu khác nhau.

7. 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

- Các đơn vị liên quan phối hợp và thành lập bộ phận chuyên môn, tổ chuyên gia đánh giá hồ sơ thiết kế hệ thống thông tin trước khi triển khai thực hiện đảm bảo đầy đủ thông tin.

Điều 10. Phát triển phần mềm thuê khoán

1. Đối với các nội dung liên quan đến việc phát triển phần mềm thuê khoán, đơn vị được thuê khoán phải đảm bảo có các tài liệu sau:

- Biên bản làm việc;

- Biên bản thống nhất nội dung công việc;

- Hợp đồng giữa các đơn vị;

- Hồ sơ liên quan đến ATTT, bảo mật của phần mềm, cơ sở dữ liệu; các cam kết đảm bảo ATTT, an ninh mạng.

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 đảm bảo ATTT

- Mã nguồn đã được nhà phát triển tự đánh giá và có biên bản kiểm thử, đánh giá đạt trước khi bàn giao cho đơn vị thuê.

- Phối hợp với đơn vị chủ quản hệ thống thông tin đánh giá mã nguồn và có phương án xử lý lỗi (nếu có).

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

Đơn vị thuê và đơn vị phát triển phối hợp thực hiện kiểm thử phần mềm trên môi trường thử nghiệm và nghiệm thu trước khi đưa vào sử dụng:

- Mã nguồn phải được đánh giá ATTT trước khi đưa vào môi trường thử nghiệm và nghiệm thu trước khi đưa vào sử dụng.

- Tất cả các lỗi liên quan đến mã nguồn (nếu có) sau khi được khắc phục, phải được đánh giá ATTT và có biên bản đánh giá trước khi đưa vào sử dụng.

4. Kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng hệ thống được đầu tư phải được kiểm định an toàn thông tin trước khi đưa vào vận hành khai thác:

- Kiểm tra hệ thống, mã nguồn có các lỗ hổng bảo mật không. Thực hiện cập nhật các bản vá ATTT hoặc nâng cấp lên phiên bản mới nhất của hãng để đảm bảo vá hoàn toàn các lỗ hổng bảo mật.

- Thực hiện nâng cấp, xử lý điểm yếu an toàn thông tin của thiết bị hệ thống trước khi đưa vào sử dụng.

- Máy chủ phải được cài đặt hệ điều hành, phần mềm nền tảng và phần mềm phòng chống mã độc có bản quyền.

5. Kiểm tra, đánh giá an toàn thông tin cho phần mềm khi thay đổi mã nguồn, kiến trúc phần mềm

Khi có thay đổi thiết kế, đơn vị thuê và đơn vị phát triển phần mềm phối hợp đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống, cần xây dựng kế hoạch trước khi có thay đổi bao gồm tối thiểu các tài liệu sau:

- Căn cứ thực hiện thay đổi (công văn, tờ trình);

- Kế hoạch chi tiết các bước thực hiện.

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

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

- Bên phát triển có cam kết không có tranh chấp về bản quyền phát triển của phần mềm.

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

Điều 11. Thử nghiệm và nghiệm thu hệ thống

1. Thử nghiệm và nghiệm thu hệ thống trước khi bàn giao và đưa vào sử dụng

Các sản phẩm, thiết bị được đầu tư trong hệ thống phải được kiểm định an toàn thông tin trước khi đưa vào vận hành khai thác:

- Kiểm tra phiên bản phần mềm cho phần cứng (firmware) các thiết bị mạng quan trọng như: Tường lửa, Switch, IDS/IPS,... xem có lỗ hổng bảo mật không. Thực hiện cập nhật các bản vá hoặc nâng cấp lên phiên bản mới nhất của hãng để đảm bảo ATTT;

- Các thiết bị hệ thống trước khi được đưa vào sử dụng phải được qua kiểm định về an ninh, an toàn, cháy nổ của các cơ quan chức năng; thực hiện nâng cấp, xử lý điểm yếu ATTT trước khi đưa vào sử dụng;

- Không cài cắm mã độc vào máy chủ; thực hiện gỡ bỏ các hệ điều hành cũ đối với máy chủ và thực hiện xóa dữ liệu (Format) đối với các ổ cứng trước khi đưa vào sử dụng.

2. Nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống

a) Hệ thống được thử nghiệm tổng thể trước khi đưa vào sử dụng và định kỳ hàng năm để đảm bảo tính an toàn, thống nhất của hệ thống.

b) Quy trình thử nghiệm hệ thống như sau:

- Phân tích yêu cầu;

- Lập kế hoạch kiểm thử;

- Thiết kế kịch bản cho quy trình kiểm thử;

- Thiết lập môi trường kiểm thử;

- Thực hiện kiểm thử;

- Đóng chu trình kiểm thử.

c) Nội dung, kế hoạch và quy trình nghiệm thu hệ thống được thực hiện theo Thông tư số 24/2020/TT-BTTTT ngày 09/09/2020 của Bộ Thông tin và Truyền thông 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.

3. Cơ quan có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống chủ quản hệ thống thông tin đảm nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống như sau:

- Kiểm thử, nghiệm thu chức năng của hệ thống;

- Kiểm thử, nghiệm thu bảo đảm an toàn thông tin;

- Kiểm thử, nghiệm thu hệ thống nội bộ của đơn vị phát triển.

4. 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

Chủ quản hệ thống thông tin có trách nhiệm phối hợp với đơn vị có chuyên trách về ATTT thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống trước khi đưa vào sử dụng.

5. Báo cáo nghiệm thu được ký xác nhận của đơn vị chuyên trách về ATTT và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng.

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

Điều 12. Quản lý an toàn mạng

1. Quản lý, vận hành, duy trì 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 (nếu có).

b) Thường xuyên kiểm tra cấu hình, các tệp 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 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.

j) Duy trì ít nhất 02 đường truyền mạng Internet từ các nhà cung cấp dịch vụ Internet khác nhau (nếu hệ thống buộc phải có kết nối mạng Internet).

k) Mật khẩu của các tài khoản thiết bị, ứng dụng, phần mềm, cơ sở dữ liệu phải được đặt mật khẩu mạn

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) Quản trị viên hệ thống quản lý, vận hành, truy cập, khai thác thông tin 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) Quản trị viên hệ thống 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 công chức, viên chức quản lý cấp trên để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm.

c) Thiết lập 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 tối ưu, tăng cường bảo mật cho thiết bị mạng, bảo mật (cứng hóa) hệ thống và nghiêm chỉnh thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác.

Điều 13. 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 đảm bảo 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) Có tài liệu liệt kê, cài đặt với những phần mềm hệ thống cài trong máy chủ.

h) Có vùng mạng quản trị riêng, giới hạn địa chỉ IP quản trị để người quản trị truy cập vào quản trị các máy chủ.

i) 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.

j) 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 đảm bảo 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 đảm bảo 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 đảm bảo 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 đảm bảo 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 đảm bảo an toàn thông tin cho các Cổng, trang thông tin điện tử

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

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.

Điều 14. 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 đảm bảo 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.

- 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.

- Lập danh sách các dữ liệu, phần mềm cần được sao lưu, có phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu

- Xây dựng tài liệu, quy trình hướng dẫn sao lưu, phục hồi dữ liệu của hệ thống: Đơn vị quản trị hệ thống thực hiện xây dựng Tài liệu hướng dẫn sao lưu cụ thể đối với từng hệ thống cung cấp dịch vụ, hệ thống điều hành mà đơn vị quản lý.

- Thực hiện sao lưu dữ liệu định kỳ: Cán bộ phụ trách sao lưu thực hiện sao lưu định kỳ theo phương án sao lưu đã được phê duyệt.

- Kiểm tra định kỳ: Dữ liệu sao lưu phải được lưu trữ an toàn và được kiểm tra thường xuyên đảm bảo sẵn sàng cho việc sử dụng khi cần. Kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu.

Điều 15. 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. Cài đặt hoặc cập nhật các bản vá cho hệ điều hành.

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 16. Quản lý phòng chống phần mềm độc hại

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

2. Các cán bộ, công chức, viên chức và người lao động trong cơ quan phải được hướng dẫn về phòng chống mã độc, các rủi ro do mã độc gây ra; không

được tự ý cài đặt hoặc gỡ bỏ các phần mềm trên máy trạm khi chưa có sự đồng ý của người có thẩm quyền theo quy định của cơ quan.

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

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

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

6. 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 17. Quản lý điểm yếu an toàn thông tin

1. Đơn vị, bộ phận phụ trách về an toàn thông tin có trách nhiệm:

a) Quản lý thông tin điểm yếu an toàn thông tin 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) Báo cáo Lãnh đạo, Cán bộ quản lý ngay khi phát hiện điểm yếu an toàn thông tin ở mức độ nghiêm trọng. Thực hiện cảnh báo và xử lý điểm yếu an toàn thông tin theo chỉ đạo. Việc xử lý điểm yếu an toàn thông tin phải bảo đảm không ảnh hưởng gián đoạn hoạt động của hệ thống.

c) Xây dựng phương án xử lý tạm thời đối với trường hợp điểm yếu an toàn thông tin chưa được khắc phục và phương án khôi phục hệ thống trong trường hợp xử lý điểm yếu thất bại.

đ) Có trách nhiệm phối hợp với đội ứng cứu sự cố, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin đối với các điểm yếu khi cần thiết.

2. Đối với hệ thống, hệ thống thành phần được đề xuất là cấp độ 3 trở lên phải thực hiện kiểm tra, đánh giá và xử lý điểm yếu an toàn thông tin 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 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.

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 và Điều 13 Thông tư số 12/2022/TT-BTTTT.

Điều 18. Quản lý sự cố an toàn thông tin

1. Phân nhóm sự cố an toàn thông tin, bao gồm:

a) Sự cố do bị tấn công mạng: Tấn công từ chối dịch vụ; tấn công giả mạo; tấn công sử dụng mã độc; truy cập trái phép, chiếm quyền điều khiển; tấn công thay đổi giao diện; tấn công mã hóa phần mềm, dữ liệu, thiết bị; phá hoại thông tin, dữ liệu, phần mềm; nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu; các hình thức tấn công mạng khác.

b) Hỏng hóc phần cứng, lỗi phần mềm của hệ thống thông tin làm mất tính sẵn sàng của hệ thống thông tin.

c) Hỏng hóc, lỗi của các hệ thống thuộc hạ tầng công nghệ thông tin, phòng máy chủ (nguồn điện, làm mát, chống sét, chống cháy...) làm mất tính sẵn sàng của hệ thống thông tin.

d) Hỏng hóc, lỗi của hệ thống mạng làm mất khả năng truy cập tới hệ thống thông tin của các đối tượng sử dụng hệ thống.

đ) Sự cố do lỗi của người quản trị, vận hành hệ thống.

e) Sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn.

2. Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin:

Đơn vị vận hành hệ thống thông tin khi phát hiện hoặc nhận được thông báo sự cố đối với hệ thống thông tin do mình quản lý, phải thực hiện:

- Ghi nhận, tiếp nhận thông báo, báo cáo sự cố và tập hợp các thông tin liên quan theo đúng quy trình;

- Phản hồi cho tổ chức, cá nhân gửi thông báo, báo cáo ban đầu ngay sau khi nhận được để xác nhận về việc đã nhận được thông báo, báo cáo sự cố;

- Chủ trì, phối hợp cùng đơn vị cung cấp dịch vụ ATTT mạng (nếu có) và các đơn vị chức năng liên quan tiến hành phân tích, xác minh, đánh giá tình hình, sơ bộ phân loại sự cố và triển khai ngay các hoạt động ứng cứu sự cố và báo cáo theo quy định;

- Báo cáo về sự cố, diễn biến tình hình ứng cứu sự cố, đề xuất hỗ trợ ứng cứu sự cố hoặc nâng cấp nghiêm trọng của sự cố (khi cần) cho chủ quản hệ thống thông tin.

3. Kế hoạch ứng phó sự cố an toàn thông tin;

a) Chủ quản HTTT chỉ đạo Đơn vị vận hành tổ chức xây dựng, phê duyệt Kế hoạch ứng phó sự cố cho các hệ thống thông tin do đơn vị trực tiếp quản lý theo đề cương tại Phụ lục II Quyết định số 05/2017/QĐ-TTg (bao gồm các điều chỉnh do Bộ Thông tin và Truyền thông ban hành nếu có) và tổ chức triển khai kế hoạch sau khi phê duyệt. Đối với các nội dung trong kế hoạch vượt thẩm quyền quyết định của đơn vị, đơn vị lấy ý kiến của đơn vị chuyên trách ATTT (đối với các nội dung yêu cầu có kinh phí), báo cáo chủ quản HTTT xem xét, quyết định

b) Các kế hoạch ứng phó sự cố sau khi được phê duyệt phải gửi đơn vị chuyên trách ATTT tổng hợp thành kế hoạch chung toàn hệ thống, trình chủ quản HTTT phê duyệt.

c) Kế hoạch ứng phó sự cố được rà soát và điều chỉnh hàng năm (nếu cần thiết) trước ngày 31 tháng 10, làm cơ sở để xây dựng kế hoạch bảo đảm an toàn thông tin năm tiếp theo.

4. Đơn vị, bộ phận phụ trách về an toàn thông tin có trách nhiệm

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

b) Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13, 14 Quyết định số 05.

c) Xây dựng và triển khai kế hoạch ứng phó sự cố an toàn thông tin theo quy định tại Điều 16 Quyết định số 05.

d) Quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về ATTT; Hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; Yêu cầu ngừng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; Phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo.

e) 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 an toàn thông tin; Yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống.

g) Tổ chức diễn tập phương án xử lý sự cố an toàn thông tin theo chỉ đạo của Lãnh đạo.

5. Trách nhiệm của người dùng

Thông tin, báo cáo kịp thời cho cán bộ chuyên trách về ATTT của cơ quan khi phát hiện các sự cố gây mất ATTT trong quá trình tham gia vào hệ thống thông tin của đơn vị; Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

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

1. Kết nối máy tính, thiết bị đầu cuối của người sử dụng vào hệ thống:

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) Đối với hệ thống thông tin có cấp độ 3 trở lên, 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. Trong quá trình 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 tỉnh hoặc đơn vị chuyên môn tổ chức.

3. 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.

Chương V
KIỂM TRA, ĐÁNH GIÁ VÀ QUẢN LÝ RỦI RO

Điều 20. 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
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	Việc sửa đổi hoặc phá hủy trái phép thông tin làm tổn hại	Việc gián đoạn truy cập hoặc sử dụng thông tin/hệ thống

	quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng	nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng	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

a) 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:

1. Thông tin Chủ quản hệ thống thông tin;

2. Thông tin Đơn vị vận hành;

3. Chức năng, nhiệm vụ, cơ cấu tổ chức của đơn vị vận hành;

4. Các cơ quan, tổ chức liên quan;

5. Phạm vi, quy mô của hệ thống.

b) 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.

- 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.

- 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 5, có xử lý thông tin bí mật nhà nước, không chấp nhận tồn tại rủi ro. Chỉ chấp nhận tồn tại các rủi ro ở mức thấp đối với hệ thống thông tin cấp độ 5 không xử lý thông tin bí mật nhà nước. Đối với hệ thống thông tin cấp độ 5, để bảo đảm tính khả thi trong việc xử lý hết các rủi ro của hệ thống, cơ quan, tổ chức cần làm rõ phạm vi của hệ thống để có biện pháp xử lý phù hợp.

+ Hệ thống thông tin cấp độ 3 hoặc cấp độ 4, 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 hoặc cấp độ 4, 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 dọa.

+ 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.

c) 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 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.

d) 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.

đ) 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

Điều 21. Kiểm tra việc tuân thủ quy định về an toàn thông tin và hiệu quả của biện pháp bảo đảm an toàn thông tin

1. Nội dung kiểm tra, đánh giá

a) Kiểm tra việc xác định cấp độ an toàn hệ thống thông tin và triển khai phương án bảo đảm an toàn thông tin; Kiểm tra hiệu quả của các biện pháp bảo đảm an toàn thông tin.

b) Kiểm tra công tác giám sát an toàn thông tin; ứng cứu sự cố an toàn thông tin.

c) Kiểm tra các nội dung khác tại Quy chế này.

2. Thẩm quyền kiểm tra

a) Các đơn vị khác tự kiểm tra trong nội bộ đơn vị.

b) Hoạt động kiểm tra về an toàn thông tin do các đơn vị thực hiện có thể lồng ghép trong chương trình kiểm tra công tác ứng dụng công nghệ thông tin hàng năm, theo kế hoạch được Lãnh đạo đơn vị phê duyệt.

Điều 22. Kết thúc vận hành, khai thác, sửa chữa, 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 VI
BÁO CÁO, CHIA SẺ THÔNG TIN

Điều 23. Chế độ báo cáo

1. Báo cáo định kỳ:

a) Báo cáo an toàn thông tin định kỳ hàng năm gồm các nội dung quy định tại khoản 3 Điều 17 Thông tư 12/2022/TT-BTTTT.

b) Báo cáo hoạt động giám sát của chủ quản hệ thống thông tin định kỳ 6 tháng theo mẫu tại Phụ lục 2 Thông tư 31/2017/TT-BTTTT.

2. Báo cáo đột xuất: Báo cáo về công tác khắc phục mã độc, lỗ hổng, điểm yếu, triển khai cảnh báo an toàn thông tin và các báo cáo đột xuất khác theo yêu cầu của các cơ quan quản lý nhà nước về an toàn thông tin.

3. Trách nhiệm lập, phê duyệt báo cáo

a) Các đơn vị chịu trách nhiệm:

- Lập báo cáo an toàn thông tin theo quy định tại điểm a khoản 1 điều này, gửi Sở Thông tin và Truyền thông trước ngày 15 tháng 11 hàng năm.

- Lập báo cáo hoạt động giám sát của chủ quản hệ thống thông tin theo quy định tại điểm b khoản 1 điều này, gửi đơn vị chuyên trách về ATTT thông trước ngày 15 tháng 6 và 15 tháng 12 hàng năm.

- Báo cáo đột xuất theo hướng dẫn của đơn vị chuyên trách ATTT.

b) Văn phòng UBND xã chịu trách nhiệm tập hợp, tổng hợp báo cáo của các đơn vị, gửi các cơ quan quản lý nhà nước về an toàn thông tin.

Chương VII
TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 24. Đơn vị vận hành - Văn phòng HĐND&UBND xã

a) Thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo quy định tại Quy chế này và các nhiệm vụ do chủ quản hệ thống thông tin phân công.

b) Chỉ đạo, phân công các bộ phận kỹ thuật thuộc đơn vị (quản lý ứng dụng; quản lý dữ liệu; vận hành hệ thống thông tin; triển khai và hỗ trợ kỹ thuật) triển khai công tác bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

Điều 25. Trách nhiệm của Phòng văn hoá và Thông tin xã

a) Thực hiện các trách nhiệm được giao tại Quy chế này.

b) Hướng dẫn triển khai Quy chế này và các quy định liên quan của Nhà nước.

c) Tổ chức triển khai thực hiện Quy chế tại các đơn vị trực thuộc.

d) Xây dựng kế hoạch, báo cáo về an toàn thông tin mạng.

Điều 26. Các đơn vị trực thuộc

a) Thực hiện trách nhiệm của chủ quản hệ thống thông tin hoặc đơn vị quản lý trực tiếp hệ thống thông tin trong trường hợp có hệ thống thông tin thuộc quản lý trực tiếp của đơn vị theo quy định của Quy chế này.

b) Tổ chức triển khai thực hiện Quy chế này tại đơn vị.

c) Thực hiện các báo cáo về an toàn thông tin mạng khi được yêu cầu.

Chương VIII
TỔ CHỨC THỰC HIỆN

Điều 27. Tổ chức triển khai Quy chế

Quy định này có hiệu lực thi hành kể từ ngày ký ban hành.

Điều 28. Rà soát, cập nhật, bổ sung Quy chế

1. Định kỳ 02 năm hoặc khi có thay đổi Quy chế bảo đảm an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung.

2. Trong quá trình thực hiện Quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời về Văn phòng HĐND & UBND xã để tổng hợp báo cáo cấp có thẩm quyền xem xét, điều chỉnh, bổ sung./

PHỤ LỤC

DANH SÁCH QUY ĐỊNH, QUY TRÌNH KÈM THEO

1. Quy định về truy cập và làm việc từ xa
2. Quy chế quản lý an toàn bảo mật hệ thống công nghệ thông tin
3. Quy định về quản lý thiết bị ngoại vi, ổ đĩa lưu trữ
4. Quy trình ứng cứu sự cố
5. Danh sách phần mềm được cài đặt trên máy trạm.

Phụ lục 01
QUY ĐỊNH QUẢN LÝ QUYỀN TRUY CẬP

1. Mục đích

Chính sách quản lý truy cập đảm bảo an toàn thông tin thông qua các biện pháp quản lý, kiểm soát việc truy cập vào thông tin và các phương tiện xử lý thông tin của HTTT theo các yêu cầu hoạt động của HTTT. Cụ thể:

a. Đảm bảo người dùng hợp lệ được truy cập và ngăn chặn những người dùng không hợp lệ truy cập tới hệ thống thông tin.

b. Ngăn chặn những người dùng trái phép truy cập và làm tổn hại hoặc ăn cắp thông tin cũng như các phương tiện xử lý thông tin.

c. Ngăn chặn các truy cập trái phép vào mạng máy tính.

d. Ngăn chặn các truy cập trái phép đến hệ thống ứng dụng.

e. Đảm bảo an toàn thông tin khi làm việc từ xa và trên các thiết bị di động.

2. Phạm vi áp dụng: Áp dụng cho Hệ thống thống thông tin tại đơn vị.

3. Nội dung

3.1. Các quy tắc kiểm soát truy cập chung

- Các nguyên tắc chung trong việc kiểm soát truy cập thông tin và các phương tiện xử lý thông tin:

+ Tất cả các thông tin quan trọng trong hệ thống CNTT đều cần phải được bảo vệ khỏi truy cập trái phép thông qua chính sách kiểm soát truy cập.

+ Quyền truy cập phải được thiết lập dựa trên nhu cầu nghiệp vụ và các yêu cầu về an toàn thông tin của HTTT.

+ Quyền truy cập cần được rà soát định kỳ.

+ Quyền truy cập cần phải được loại bỏ khi không còn nhu cầu sử dụng.

+ Các thủ tục kiểm soát truy cập cần phải có chế độ ghi lại nhật ký khi một người sử dụng truy cập vào hệ thống thông tin quan trọng.

a) Quy tắc quyền tối thiểu

1. Việc cấp quyền truy cập phải đảm bảo thông tin chỉ được cung cấp một cách tối thiểu cho những người sử dụng nhằm đáp ứng đủ yêu cầu nghiệp vụ được giao.

b) Quy tắc cấp quyền truy cập

- Cần phải xây dựng, ban hành quy trình cấp phép truy cập hệ thống CNTT.

- Quản lý quyền truy cập của cán bộ HTTT:

+ Khi có nhân viên mới, bộ phận quản lý trực tiếp nhân viên mới cần phải thông báo cho nhóm quản lý truy cập (thuộc Văn phòng HĐND và UBND xã), để tiến hành cấp quyền.

+ Khi có cán bộ thôi việc, nghỉ việc hoặc thuyên chuyển công tác, bộ phận quản lý nhân sự chịu trách nhiệm thông báo kịp thời cho nhóm Quản lý truy cập (thuộc Văn phòng HĐND và UBND xã) để tiến hành thu hồi quyền truy cập.

- Quản lý quyền truy cập của người dùng từ xa:

+ Người dùng từ xa muốn truy cập hệ thống CNTT của HTTT phải có đề xuất bằng văn bản của đơn vị đang làm việc trực tiếp với người dùng từ xa gửi tới nhóm Quản lý truy cập (thuộc Văn phòng HĐND và UBND xã) cùng phối hợp để trình cấp có thẩm quyền phê duyệt.

+ Chỉ cấp quyền cho người dùng từ xa khi được phê chuẩn của cấp có thẩm quyền.

+ Khi hết nhu cầu sử dụng: người dùng từ xa, đơn vị phối hợp với người dùng từ xa phải có trách nhiệm thông báo kịp thời cho nhóm Quản lý truy cập (thuộc Văn phòng HĐND và UBND xã) để tiến hành thu hồi quyền truy cập.

c) Quy tắc trao quyền

- Chỉ nhóm Quản lý truy cập (thuộc Văn phòng HĐND và UBND xã), bộ phận quản trị hệ thống CNTT, bộ phận quản trị ứng dụng được phép cấp quyền truy cập vào hệ thống thông tin.

- Văn phòng HĐN và UBND xã có trách nhiệm giám sát và theo dõi việc cấp phát quyền truy cập.

d) Quy tắc cấu hình truy cập mặc định

- Phải có cấu hình truy cập mặc định thỏa mãn điều kiện:

+ Từ chối tất cả các đối tượng truy cập chưa đăng ký đến hệ thống thông tin và tài nguyên thông tin.

+ Nếu không có chỉ dẫn phân quyền cụ thể, các đối tượng đều phải áp dụng quyền này.

+ Có chế độ ghi lại nhật ký khi có truy cập không đăng ký.

3.2. Kiểm soát truy cập vật lý

Dùng các biện pháp vật lý như: Hàng rào, cửa, khóa, bảo vệ, camera, chuông báo động, hệ thống phát hiện di chuyển...(tham chiếu trong Quy chế ATTT mục Bảo mật vật lý và môi trường) để kiểm soát truy cập mức vật lý vào tài nguyên của HTTT.

- Phải kiểm soát nhân viên ra vào các khu vực quan trọng như phòng máy chủ, nơi làm việc (tham chiếu Nội quy các khu vực bảo mật).

- Phải kiểm soát khách ra vào các khu vực quan trọng (tham chiếu Hướng dẫn ra vào khu vực làm việc).

3.3. Kiểm soát truy cập logic

Dùng các biện pháp kỹ thuật hoặc hành chính để kiểm soát truy cập vào hệ thống thông tin và phương tiện xử lý thông tin (ví dụ: hệ thống mạng máy tính, hệ điều hành, hệ thống ứng dụng…) của HTTT.

a) Quản lý truy cập người dùng

- Đăng ký sử dụng: Phải có quy trình chính thức cho việc đăng ký để thực hiện cấp phát truy cập, thay đổi quyền truy cập và việc hủy bỏ đăng ký truy cập để thu hồi quyền truy cập trên tất cả các hệ thống và dịch vụ thông tin.

- Quản lý đặc quyền: Cần phải giới hạn và kiểm soát việc cấp phát và sử dụng các đặc quyền bằng văn bản hoặc các biện pháp kỹ thuật (nếu có) đối với mỗi hệ thống.

- Quản lý mật khẩu và tài khoản: Cần phải có văn bản quy định việc quản lý, sử dụng mật khẩu và tài khoản.

- Xem xét lại quyền truy cập người dùng: Cần phải có quy trình chính thức cho việc rà soát định kỳ các quyền truy cập của người sử dụng.

b) Trách nhiệm của người dùng

- Sử dụng mật khẩu: Người dùng cần tuân thủ các quy tắc sử dụng và đặt mật khẩu an toàn trong Quy định quản lý và sử dụng tài khoản, mật khẩu.

- Các thiết bị không được theo dõi: Cần đảm bảo rằng các thiết bị khi không được theo dõi phải được bảo vệ thích hợp.

- Chính sách bàn sạch và màn hình sạch: Không để tài liệu trên bàn khi không ở chỗ ngồi, khóa màn hình khi đi ra ngoài, thực hiện theo chính sách Bàn sạch/Màn hình sạch. Bàn sạch/Màn hình sạch là cách để ngăn ngừa các nguy cơ lộ thông tin, truy cập trái phép, mất thông tin.

c) Kiểm soát truy cập mạng

- Chính sách sử dụng các dịch vụ mạng: Người dùng chỉ được cung cấp quyền truy cập vào các dịch vụ mà họ đã được cấp phép. Cần phải có văn bản quy định về việc kiểm soát và quản lý truy cập mạng máy tính.

- Xác thực người sử dụng qua các kết nối bên ngoài: Phải sử dụng các biện pháp xác thực thích hợp để quản lý truy cập từ bên ngoài.

- Định danh các thiết bị trong mạng: Cần phải có biện pháp nhận biết các thiết bị kết nối vào hệ thống mạng máy tính.

- Bảo vệ các cổng mạng cho phép cấu hình và kết nối từ xa: Cần phải có biện pháp kiểm soát các truy cập logic và vật lý tới các cổng dùng cho việc cấu hình hoặc kết nối vào hệ thống mạng máy tính.

- Phân tách các mạng: Cần phải phân tách mạng theo các nhóm người dùng, dịch vụ mà mạng cung cấp hoặc theo tính chất đặc thù của hệ thống thông tin có trên mạng. Cần phải có văn bản chỉ rõ các vùng mạng được phân tách.

- Kiểm soát kết nối mạng máy tính: Đối với các mạng, đặc biệt là các mạng mở rộng ra ngoài tổ chức, số lượng người sử dụng có thể kết nối đến cần phải được giới hạn để đảm bảo an toàn và phù hợp với các yêu cầu nghiệp vụ. Cần phải có văn bản quy định kiểm soát các kết nối tại các vùng mạng chính của HTTT (ví dụ: internet, WAN, intranet…).

- Quản lý luồng thông tin trên mạng: Cần phải có biện pháp kiểm soát và hạn chế lưu lượng mạng chỉ để đáp ứng các yêu cầu nghiệp vụ. Cần phải có văn bản chỉ ra các lưu lượng mạng nào cần cho yêu cầu nghiệp vụ.

d) Kiểm soát truy cập hệ điều hành

- Cần phải có Quy định kiểm soát truy cập hệ điều hành.

- Đăng nhập an toàn: Cần phải có biện pháp đăng nhập an toàn vào hệ điều hành. Cần phải có văn bản quy định các quy tắc đăng nhập an toàn hệ điều hành.

- Định danh và xác thực người dùng: Mỗi người dùng chỉ được có một định danh duy nhất để sử dụng cho mỗi mục đích. Cần phải có biện pháp để xác thực người dùng.

- Hệ thống quản lý mật khẩu: Cần phải có biện pháp quản lý mật khẩu nhằm bảo đảm việc sử dụng, lưu trữ và quản lý mật khẩu được an toàn. Cần phải có văn bản quy định về quản lý mật khẩu.

- Sử dụng các tiện ích hệ thống: Các chương trình tiện ích của hệ điều hành phải được hạn chế và kiểm soát một cách chặt chẽ. Cần phải có văn bản chỉ rõ các chương trình tiện ích được phép sử dụng.

- Thời gian giới hạn của phiên làm việc: Cần phải có biện pháp ngắt các phiên làm việc không hoạt động sau một khoảng thời gian nhất định.

- Giới hạn thời gian kết nối: Cần phải có văn bản quy định thời gian được phép kết nối để đảm bảo an toàn cho các ứng dụng có mức rủi ro cao.

e) Kiểm soát truy cập ứng dụng và thông tin

- Hạn chế truy cập thông tin: Cần phải có biện pháp kiểm soát truy cập tới thông tin và các chức năng của hệ thống ứng dụng.

- Cách ly hệ thống quan trọng: Cần phải cách ly các hệ thống quan trọng với môi trường bình thường.

f) Kiểm soát truy cập khi làm việc từ xa và trên các thiết bị di động

- Làm việc trên các thiết bị di động: Cần phải có văn bản quy định nhằm đảm bảo an toàn thông tin khi làm việc trên các thiết bị di động.

- Làm việc từ xa: Các điểm làm việc từ xa cần phải được cấp phép, đảm an toàn vật lý cho môi trường và tuân thủ các chính sách, quy định an toàn của HTTT.

4. Ngoại lệ

Tất cả các trường hợp ngoại lệ phải được xem xét và phê duyệt bởi Lãnh đạo.

5. Kiểm tra tuân thủ và kỷ luật

- Văn phòng HĐND và UBND xã có trách nhiệm kiểm tra việc tuân thủ các nội dung của quy trình này.

- Tất cả các trường hợp vi phạm sẽ bị kỷ luật theo Quy định Khen thưởng và xử phạt của HTTT.

Phụ lục 02
QUY TRÌNH QUẢN LÝ MẠNG RIÊNG ẢO

MỤC ĐÍCH

Quy trình quản lý mạng riêng ảo (VPN) dành cho người dùng từ xa mô tả các bước đề xuất, xem xét, phê duyệt, thực hiện, theo dõi và quản lý các truy cập từ xa ứng dụng công nghệ VPN dành cho các người dùng từ xa sử dụng VPN để kết nối với hệ thống thông tin do đơn vị quản lý.

Giúp tổ chức theo dõi, kiểm soát và quản lý các truy cập từ bên ngoài, đảm bảo các yêu cầu về an ninh, an toàn thông tin thuộc lĩnh vực CNTT trong hoạt động thông tin của đơn vị.

PHẠM VI ÁP DỤNG

Quy trình này áp dụng để thực hiện việc cấp phép và quản lý các truy cập từ xa ứng dụng công nghệ Mạng riêng ảo (VPN) đối với người dùng từ xa của đơn vị.

Quy trình này có liên quan tới:

- Các cán bộ nhân viên của Văn phòng HĐND&UBND xã
- Các cán bộ nhân viên của Phòng, ban
- Và các phòng chức năng liên quan khác

NỘI DUNG

Lưu đồ quy trình

Bước	Trách nhiệm	Công việc	Mô tả/ biểu mẫu/Tài liệu tham chiếu
	Lãnh đạo đơn vị đề nghị	Đề nghị cấp phép/ thu hồi truy cập VPN	Đề nghị cấp phép/ thu hồi quyền truy cập VPN
1	Lãnh đạo đơn vị đề nghị	-Xác định thời gian, quyền hạn truy cập/ thu hồi CA -Cam kết bảo mật (đối với bên thứ 3)	Đề nghị cấp phép/ thu hồi quyền truy cập VPN
2	Ban lãnh đạo	Duyệt	
3	Văn phòng HĐND và UBND	Hỗ trợ cài đặt VPN client	

4	Văn phòng HĐND và UBND	Tạo và cấp OTP/ Thu hồi CA. Cấp phếp truy cập VPN	
5	Văn phòng HĐND và UBND	Báo cáo/ lưu hồ sơ	
6	Văn phòng HĐND và UBND	Gia hạn CA khi hết hiệu lực	

Diễn giải quy trình

Bước	Các bước thực hiện	Nội dung thực hiện
	Đề nghị cấp phép/ thu hồi truy cập VPN	- Lãnh đạo đơn vị có yêu cầu cấp phép/ thu hồi truy cập VPN gửi đề nghị bằng văn bản/email tới Lãnh đạo đơn vị
1	Xác định thời gian, quyền hạn truy cập/ thu hồi CA	- Lãnh đạo đơn vị có yêu cầu cấp phép/ thu hồi VPN cần xác định chính xác thời hạn và quyền hạn truy cập VPN. - Trường hợp cấp phép cho bên thứ 3: cần yêu cầu bên thứ 3 làm biên bản thỏa thuận bảo mật thông tin.
2	Duyệt	- Lãnh đạo đơn vị sẽ tiến hành xem xét đề nghị và phê duyệt đồng ý hoặc từ chối - Nếu đồng ý đề nghị: Tiến hành bước 3 - Nếu không đồng ý: trả lời đơn vị đề nghị và đưa ra các yêu cầu cần thay đổi, bổ sung
3	Hỗ trợ cài đặt VPN client	- Cán bộ Văn phòng HĐND&UBND xã tiến hành hướng dẫn và hỗ trợ người dùng cài đặt VPN Client
4	Tạo và cấp OTP/ Thu hồi CA. Cấp phép truy cập VPN	- Cán bộ quản trị tiến hành tạo tài khoản OTP và gửi đến người sử dụng qua email - Trường hợp đề nghị thu hồi CA thì cán bộ quản trị ATTT sẽ tiến hành xác định và thu hồi quyền truy cập VPN - Văn phòng HĐND&UBND xã sẽ cấp phép truy cập VPN theo đề nghị được phê duyệt.
5	Báo cáo/ lưu hồ sơ	Báo cáo Lãnh đạo và lưu lại hồ sơ.
6	Gia hạn CA khi hết hiệu lực	- Khi hết thời hạn sử dụng của CA đã được cấp, các đơn vị cần đề nghị danh sách cấp lại/ gia hạn CA theo trình tự từ Bước 1. Mặc định thời hạn có hiệu lực của CA là 1 năm

c) Hồ sơ lưu

Stt	Tên hồ sơ lưu	Mã số	Nơi lưu
	Danh sách cài đặt VPN dành cho người dùng từ xa bên ngoài	BM.ISMS.xxx/DSVPN/ATMTT	P.QLATMTT

4. Ngoại lệ

Tất cả các trường hợp ngoại lệ phải được xem xét và phê duyệt bởi Lãnh đạo đơn vị.

5. Kiểm tra tuân thủ và kỷ luật

Bộ phận phụ trách an toàn thông tin có trách nhiệm kiểm tra việc tuân thủ Quy trình quản lý truy cập VPN dành cho người dùng từ xa.

Tất cả các trường hợp vi phạm sẽ bị kỷ luật theo Quy định Khen thưởng và xử phạt của đơn vị.

Phụ lục 03
QUY ĐỊNH AN TOÀN THÔNG TIN VÀ PHẦN MỀM CHO MÁY TRẠM

Chương I
QUY ĐỊNH CHUNG

1. Mục đích

Quy định các yêu cầu trong việc thiết lập cấu hình đối với phần cứng, hệ điều hành, phần mềm cài đặt cho máy tính cá nhân để đảm bảo tính bảo mật và an toàn thông tin.

2. Đối tượng và Phạm vi áp dụng

a) Quy định áp dụng cho các máy tính cá nhân được sử dụng trong đơn vị.

b) Quy định này được áp dụng cho các nghiệp vụ triển khai, cài đặt, thiết lập chính sách, kiểm tra tuân thủ và kiểm toán đối với máy tính cá nhân.

3. Trách nhiệm bộ phận hỗ trợ

Bộ phận hỗ trợ tại các đơn vị có nhiệm vụ triển khai cài đặt, kiểm tra các máy tính cá nhân bao gồm:

a) Triển khai, cài đặt các thành phần trên máy tính các nhân đáp ứng theo quy định tiêu chuẩn an ninh thông tin cài đặt trên máy tính cá nhân.

b) Đảm bảo cập nhật các bản vá lỗi cho hệ điều hành và các ứng dụng nghiệp vụ.

c) Kiểm tra tuân thủ, kiểm toán định kỳ các máy tính cá nhân tại đơn vị mình và báo cáo cho lãnh đạo đơn vị hiện trạng cài đặt máy tính cá nhân.

CHƯƠNG II
QUẢN LÝ VÀ CẤU HÌNH MÁY TÍNH CÁ NHÂN

1. Quy định về cài đặt/gỡ bỏ phần mềm trên máy trạm

a) Máy tính cá nhân tự trang bị phải được sự đồng ý của lãnh đạo đơn vị trước khi đưa vào sử dụng.

b) Tất cả máy tính cá nhân phải được bộ phận hỗ trợ tại đơn vị cài đặt phần mềm. Việc cài đặt, cấu hình bảo mật đối với máy tính cá nhân phải đảm bảo:

- Chỉ cài đặt hệ điều hành tiêu chuẩn trên phân vùng riêng biệt.

- Chỉ cho phép khởi động từ ổ đĩa cứng cài hệ điều hành.

- Phải được thiết lập tắt các tính năng tự động thực thi (Autorun) trên tất cả các ổ đĩa.

- Phải được cấu hình ngăn chặn thực thi trực tiếp những file script (JS, JSE, OTF, REG, SCT, SHB, SHS, VB, VBE, VBS, WSC, WSF, WSH).

- Các tài khoản người dùng không sử dụng phải được gỡ bỏ (ví dụ: tài khoản Guest)

c) Việc quản lý và phân quyền truy cập thông tin và ứng dụng phù hợp với chức năng nhiệm vụ của người sử dụng.

- Phân quyền truy cập đến từng thư mục, chức năng của chương trình.

- Phân quyền đọc, ghi, xóa, thực thi đối với thông tin, dữ liệu, chương trình.

d) Máy tính cá nhân chỉ được cài đặt các phần mềm phục vụ cho công việc như các phần mềm văn phòng, các phần mềm nghiệp vụ theo đúng "danh sách các phần mềm được phép cài đặt cho máy tính cá nhân của đơn vị" (*phụ lục 1 gửi kèm*).

e) Không lưu trữ các bộ cài phần mềm có file crack, keygen, patch trong máy tính. Cá nhân tự chịu trách nhiệm về các phần mềm cài đặt trên máy tính, tuyệt đối không được cài đặt các phần mềm có tính chất gây hại hoặc giám sát hệ thống (nghe trộm, thăm dò, ăn cắp thông tin).

f) Các đơn vị căn cứ chức năng, nghiệp vụ, quy trình sử dụng có thể cập nhật danh sách các phần mềm được phép cài đặt tại đơn vị mình.

g) Đối với phần mềm có nhu cầu cài đặt thêm ngoài danh sách, việc cài đặt phải được sự đồng ý của lãnh đạo đơn vị.

3. Quy định về phần mềm an ninh (chống mã độc, chống tấn công)

a) Tất cả các máy tính cá nhân phải cài đặt các phần mềm phòng, chống mã độc tập trung.

b) Phần mềm phòng, chống mã độc và ngăn chặn tấn công phải được kích hoạt khi cài đặt và được cấu hình định kỳ cập nhật dấu hiệu nhận biết virus, mã độc mới nhất.

c) Việc kiểm tra, diệt virus, mã độc cho máy tính cá nhân phải được thực hiện thường xuyên liên tục, ít nhất 01 lần/tuần.

d) Người dùng phải báo ngay cho người quản trị hệ thống xử lý trong trường hợp phát hiện nhưng không diệt được virus, mã độc.

4. Quy định về sử dụng thiết bị quang học và lưu trữ di động (CD, DVD, CDROM, USB, thẻ nhớ, ổ cứng di động)

a) Máy tính cá nhân được đơn vị trang bị mới phải gỡ bỏ vật lý các ổ đĩa CD/DVD/CDROM.

b) Đối với máy tính cá nhân có nhu cầu lắp đặt các ổ đĩa CD/DVD/CDROM, việc lắp đặt phải được sự đồng ý của lãnh đạo đơn vị.

c) Tất cả các thiết bị lưu trữ thông tin di động như USB, ổ cứng di động, thẻ nhớ hoặc tất cả các thiết bị lưu trữ thông tin di động khác phải thực hiện diệt virus trước khi sử dụng.

5. Quy định gỡ bỏ các thành phần không sử dụng

Các thành phần không sử dụng phải được gỡ bỏ. Bao gồm các thành phần như sau:

- Các trò chơi mặc định trên máy.
- IIS Admin Service
- World Wide Web Publishing Services
- NetMeeting Remote Desktop Sharing
- Routing and Remote Access
- Simple Network Management Protocol (SNMP) Service.
- Simple Network Management Protocol (SNMP) Trap
- Simple Service Discovery Protocol (SSDP) Discovery Service.

6. Quy định về quản lý bản vá lỗi

Tất cả các máy tính cá nhân đều phải được cập nhật đầy đủ, kịp thời các bản vá bao gồm nhưng không giới hạn:

- Hệ điều hành.
- Các phần mềm văn phòng.
- Các phần mềm chuyên môn nghiệp vụ.

7. Quy định về việc quản lý truy cập hệ điều hành

Quy định về kiểm soát truy cập hệ điều hành phải đáp ứng các yêu cầu sau:

a) Mỗi người sử dụng hệ điều hành phải có một định danh duy nhất và được xác thực, nhận dạng, lưu vết khi truy cập hệ điều hành.

b) Sử dụng các phương pháp xác thực khác như sinh trắc học (vân tay) hoặc thẻ đối với các máy chủ quan trọng ngoài việc xác thực bằng mật khẩu.

CHƯƠNG III
SỬ DỤNG MÁY TÍNH CÁ NHÂN

1. Quy định về sử dụng Internet

a) Nhân viên không được phép truy cập vào các trang web có nội dung đồi trụy, phản động vi phạm pháp luật Việt Nam.

b) Không được tự ý tổ chức và tham gia hội thảo về các vấn đề chính trị, kinh tế, văn hóa, xã hội liên quan đến Việt Nam trên Internet; chỉ được tham gia các diễn đàn và hội thảo trên Internet liên quan đến đơn vị sau khi được sự chấp

thuận của Lãnh đạo theo quy định của đơn vị về việc cung cấp tin tức ra bên ngoài.

c) Nhân viên không được thực hiện các hình thức Brute Force, DOS hoặc sử dụng bất kỳ công cụ tấn công các trang web nội bộ và bên ngoài Internet.

d) Nhân viên chịu trách nhiệm về việc truy cập, đăng tải nội dung trên Internet.

2. Quy định về truy cập (tài khoản, mật khẩu)

Việc sử dụng các mật khẩu đăng nhập máy tính phải tuân theo các quy định sau:

a) Tuân thủ đầy đủ về cách đặt mật khẩu, thiết lập mật khẩu và quản lý mật khẩu theo quy định về An toàn bảo mật trong mạng hoạt động quản lý nhà nước của đơn vị.

b) Nếu cần quản lý nhiều mật khẩu, cần sử dụng chương trình quản lý mật khẩu, không ghi mật khẩu ra giấy, ra file không mã hóa.

c) Khi kết nối vào thiết bị mạng (console, telnet...) xong phải tắt các phiên làm việc có sử dụng mật khẩu.

e) Khi bị lộ mật khẩu, hoặc nghi ngờ mật khẩu bị lộ phải đổi mật khẩu và báo lại ngay với người có trách nhiệm (không để quá 1 tiếng đồng hồ kể từ lúc phát sinh sự cố).

f) Khi được cung cấp mật khẩu mới hoặc được reset mật khẩu, cần phải đổi ngay mật khẩu mới.

f) Trường hợp đặc biệt: Một số dịch vụ mạng quan trọng, hệ thống đặc biệt thì ngoài mật khẩu, các dịch vụ, hệ thống này còn được thiết lập thêm biện pháp chứng thực mạnh như: Thông tin sinh trắc học (vân tay, …), chữ ký số, mật khẩu dùng 1 lần (OTP - One Time Password). Đối với các biện pháp chứng thực mạnh kể trên, người sử dụng không được cho mượn khóa chứa chữ ký số (Smart Card, Smart Key), thiết bị OTP mà mình quản lý.

3. Quy định về an toàn vật lý (khoá máy, bảo vệ laptop khi di chuyển).

a) Quy định về việc khóa màn hình máy tính (clear screen)

- Máy tính phải được cài screen saver tối đa 05 phút (trừ các máy tính dùng để giám sát hệ thống)

- Người sử dụng luôn phải khóa màn hình hoặc thoát (log out/off) hoặc tắt máy khi rời vị trí làm việc.

b) Quy định về việc lưu trữ tài liệu, dữ liệu (clear desk)

- Các tài liệu quan trọng (hợp đồng, tài liệu nghiên cứu…) và các thiết bị lưu trữ thông tin di động (USB, ổ cứng di động, thẻ nhớ…) chứa dữ liệu quan trọng cần được lưu trữ tại vị trí có kiểm soát (ngăn kéo có khóa, két sắt…).

4. Quy định khi chuyển giao hoặc thanh lý máy tính cá nhân

- Người dùng không được cho người khác mượn hoặc sử dụng máy tính của mình mà không kiểm soát.

- Máy tính cá nhân khi chuyển giao hoặc thanh lý phải đảm bảo dữ liệu cũ của người sử dụng trước trên thiết bị lưu trữ, xử lý thông tin được xóa bỏ một cách đúng đắn và không thể phục hồi nhằm tránh lộ thông tin ngoài ý muốn.

5. Quy định đối với máy tính cá nhân không phải là tài sản của đơn vị có nhu cầu sử dụng tại đơn vị

- Máy tính cá nhân không phải là tài sản của đơn vị có nhu cầu sử dụng tại đơn vị phải đảm bảo các yêu cầu sau:

+ Được phê duyệt bởi lãnh đạo đơn vị hoặc người được ủy quyền.

+ Được cài đặt phần mềm antivirus, cập nhật dấu hiệu nhận biết mã độc mới nhất. Phần mềm antivirus phải được kích hoạt tự động bảo vệ, kiểm tra, phát hiện, xử lý mã độc khi có kết nối đến thiết bị ngoại vi hoặc tải dữ liệu từ Internet.

+ Chỉ được cài đặt chỉ mở các cổng truy cập phục vụ cho công việc, không được kết nối tới khu vực thông tin, dữ liệu nội bộ của đơn vị như: hệ thống cơ sở dữ liệu, máy chủ chia sẻ dữ liệu, mạng điều hành sản xuất kinh doanh.

6. Quy định làm việc từ xa

a) Cá nhân phải có trách nhiệm đảm bảo an toàn thông tin và dữ liệu của đơn vị bao gồm thiết bị truy cập từ xa của đơn vị và của cá nhân.

b) Nhân viên chỉ được sử dụng quyền truy cập từ xa khi có nhu cầu xử lý công việc của đơn vị, không được sử dụng quyền truy cập từ xa cho mục đích riêng.

c) Nhân viên cần áp dụng tối thiểu các biện pháp sau để hạn chế thiệt hại đến mức thấp nhất khi có xảy ra sự cố:

- Thiết bị truy cập từ xa nên có chế độ mã hóa dữ liệu trên ổ cứng.

- Thiết bị truy cập từ xa cần phải đặt mật khẩu an toàn (áp dụng theo điều 12 của Quy định này).

- Không lưu trữ tài khoản hoặc mật khẩu truy cập hệ thống cơ quan trong thiết bị truy cập từ xa hoặc phải lưu trữ dưới hình thức mã hóa.

- Thiết bị truy cập từ xa nên cài đặt chế độ cấp nhật bản vá lỗi cho hệ điều hành và phần mềm hàng ngày.

- Thiết bị truy cập từ xa phải hỗ trợ, cài đặt, sử dụng VPN khi làm việc từ xa.

CHƯƠNG IV
ĐIỀU KHOẢN THI HÀNH

1. Kiểm tra tuân thủ và kỷ luật

a) Đơn vị phụ trác ATTT có trách nhiệm kiểm tra việc tuân thủ Quy định này.

b) Tùy vào mức độ nghiêm trọng của hành vi vi phạm, Lãnh đạo đơn vị sẽ quyết định các hình thức xử lý tương.

c) Với các hành vi vi phạm, xử lý theo các quy định về xử lý kỷ luật của đơn vị.

2. Triển khai thực hiện

a) Tài liệu này có hiệu lực kể từ ngày ký;

b) Đơn vị phụ trác ATTT có trách nhiệm tổ chức hướng dẫn phối hợp với các đơn vị liên quan thực hiện tài liệu này;

c) Việc sửa đổi, bổ sung, thay thế tài liệu này do trưởng Bộ phận phụ trách ATTT thực hiện và trình Lãnh đạo đơn vị phê duyệt.

Phụ lục 04

QUY TRÌNH XỬ LÝ SỰ CỐ AN TOÀN THÔNG TIN MẠNG

1. Mục đích

Tài liệu này hướng dẫn các bước thực hiện xử lý sự cố an toàn thông tin tại UBND xã Chà Tở tỉnh Điện Biên khi có phát sinh.

2. Phạm vi áp dụng

Áp dụng cho toàn đơn vị và các đơn vị trực thuộc.

3. Thuật ngữ và định nghĩa

- LĐĐV: Lãnh đạo đơn vị.

- Phishing: là hành vi giả mạo như là một thực thể đáng tin cậy (website của các cơ quan, tổ chức, các website xã hội phổ biến, các trung tâm chi trả trực tuyến,…) để lấy cắp thông tin nhạy cảm như tên người dùng, mật khẩu, các chi tiết thẻ tín dụng… thông qua các giao tiếp trên mạng.

- Deface: Là tấn công thay đổi nội dung website của nạn nhân thông qua lỗ hổng bảo mật.

- Phát tán Malware: là hành vi phát tán các phần mềm độc hại (virus, trojan, backdoor…) qua môi trường internet.

- DoS (Denial of Service) - tấn công từ chối dịch vụ bằng cách chiếm dụng một lượng lớn tài nguyên mạng, tài nguyên hệ thống như băng thông, bộ nhớ, khả năng xử lý … và làm mất khả năng đáp ứng yêu cầu dịch vụ từ các khách hàng khác.

4. Nội dung quy trình

4.1 Sơ đồ quy trình

Người chịu trách nhiệm	Trình tự công việc	Tài liệu liên quan
Văn phòng HĐND&UBND xã	Tiếp nhận sự cố	- Cảnh báo sự cố (Công văn, email, điện thoại, website) - Phát hiện sự cố thông qua kiểm tra, rà soát, đánh giá
Văn phòng HĐND&UBND xã/ Đơn vị tư vấn, triển khai	Xác minh/ xác nhận sự cố	- Xem xét tình trạng, mức độ, phạm vi và độ ưu tiên xử lý
Văn phòng HĐND&UBND xã/ Đơn vị tư vấn, triển khai	Phân loại sự cố	- Sự cố về tấn công thay đổi giao diện (deface) - Sự cố về tấn công lừa đảo - Sự cố về tấn công phát tán mã độc (malware) - Sự cố về một số tấn công mạng - Sự cố có yếu tố nước ngoài - Sự cố tấn công khác
Lãnh đạo đơn vị (LĐĐV)	Báo cáo LĐĐV và Trung tâm giám sát ATTT Điện Biên	- Chỉ đạo xử lý và phân công trách nhiệm xử lý
Văn phòng HĐND&UBND xã/ Đơn vị tư vấn, triển khai	Thu thập thông tin để phục vụ phân tích sự cố	- Thông tin về đầu mối liên hệ - Thu thập thông tin hệ thống - Thu thập chức năng của hệ thống - Thu thập cấu hình của hệ thống (OS, servise, version,network, …) - Thu thập chứng cứ, - Thu thập bộ nhớ - Thu thập trạng thái network và kết nối - Thu thập các tiến trình đang chạy - Thu thập hard drive media - Thu thập removeble media - Thu thập log file

Văn phòng HĐND&UBND xã/ Đơn vị tư vấn, triển khai	Phân tích sự cố	- Phân tích dòng thời gian - Thời gian bị sửa đổi, truy cập, tạo hoặc thay đổi. - Thời gian thực hiện các cập nhật lớn đối với hệ thống - Thời điểm mà hệ thống sử dụng lần cuối cùng - Phân tích dữ liệu
Văn phòng HĐND&UBND xã/ Đơn vị tư vấn, triển khai	Xử lý sự cố	- Gỡ bỏ sự cố - Xác định và gỡ bỏ các backdoors - Phân tích và kiểm tra lỗ hổng sau khi thực hiện các bản vá lỗi - Khôi phục dữ liệu - Thu thập các tập tin, hình ảnh, email, … bị xóa, thời gian bị xóa - Tìm kiếm các tập tin không thể khôi phục - Khôi phục các tập tin phù hợp
Văn phòng HĐND&UBND xã/ Đơn vị tư vấn, triển khai	Tổng hợp báo cáo LĐĐV và Trung tâm giám sát ATTT Điện Biên	- Báo cáo kết quả phân tích sự cố: mô tả chi tiết các bước quan trọng khi thực hiện xử lý sự cố. - Tổng hợp báo cáo gửi Lãnh đạo cơ quan, tổ chức và các bên liên quan đến sự cố - Rút kinh nghiệm và ứng dụng cho các sự cố tương tự
Văn phòng HĐND&UBND xã, Trung tâm giám sát ATTT Điện Biên, Các bên liên quan	Lưu hồ sơ	

4.2 Mô tả quy trình

4.2.1 Tiếp nhận sự cố

Văn phòng HĐND&UBND xã tiếp nhận thông tin về sự cố qua các phương thức: Email, điện thoại, công văn … Bên cạnh đó Văn phòng nhận được các thông báo sự cố từ các hệ thống giám sát của các cơ quan nhà nước có thẩm quyền (Sở Thông tin và Truyền thông hoặc Trung tâm giám sát ATTT Điện Biên).

4.2.2 Xác minh/xác nhận sự cố

Văn phòng HĐND&UBND xã hoặc đơn vị tư vấn, triển khai tiến hành xác minh, xác nhận sự cố bao gồm các thông tin như sau:

- Tình trạng (Sự cố sẽ xãy ra; Sự cố đang xảy ra; Sự cố đã xảy ra);

- Mức độ (Sự cố nghiêm trọng; Sự cố bình thường);

- Phạm vi (Sự cố diện rộng; Sự cố mạng máy tính; Sự cố một máy tính);

- Và địa điểm xảy ra sự cố.

4.2.3 Phân loại sự cố

Sau khi xác nhận được sự cố, Văn phòng HĐND&UBND xã hoặc đơn vị tư vấn, triển khai có trách nhiệm phân loại các sự cố theo hình thức như sau:

- Sự cố về tấn công thay đổi giao diện (deface);

- Sự cố về tấn công lừa đảo (phishing);

- Sự cố về tấn công phát tán mã độc (malware);

- Sự cố về tấn công từ chối dịch vụ (DoS/DDoS);

- Sự cố có yếu tố nước ngoài (hợp tác quốc tế);

- Sự cố tấn công khác.

4.2.4 Báo cáo LĐĐV, xin ý kiến chỉ đạo

Ngay sau khi phân loại được sự cố Văn phòng HĐND&UBND xã có trách nhiệm báo cáo Lãnh đạo đơn vị để xem xét loại sự cố và tuỳ theo đối tượng sẽ tiến hành phân công cho các thành viên trong bộ phận chuyên trách xử lý và báo cáo Lãnh đạo đơn vị.

Các trường hợp phức tạp không tự xử lý được, gửi công văn nhờ sự hỗ trợ của các đơn vị chuyên trách về công nghệ thông tin và Trung tâm giám sát ATTT Điện Biên.

4.2.5 Thu thập thông tin phục vụ phân tích sự cố

Văn phòng HĐND&UBND xã hoặc đơn vị tư vấn, triển khai phối hợp các đơn vị liên quan tiến hành thu thập các thông tin:

- Thông tin về đầu mối liên hệ

- Thu thập thông tin hệ thống

- Thu thập chức năng của hệ thống

- Thu thập cấu hình của hệ thống (Hệ điều hành, dịch vụ, phiên bản, kết nối mạng….

- Thu thập chứng cứ

- Thu thập bộ nhớ

- Thu thập trạng thái network và các kết nối

- Thu thập các tiến trình đang chạy

- Thu thập nhật ký hệ thống (Log file)

4.2.6 Phân tích sự cố

Văn phòng HĐND&UBND xã hoặc đơn vị tư vấn, triển khai tiến hành phân tích sự cố, bao gồm các thông tin sau:

- Phân tích dòng thời gian

- Thời gian bị sửa đổi, truy cập, tạo hoặc thay đổi

- Thời gian thực hiện các cập nhật lớn đối với hệ thống

- Thời điểm mà hệ thống sử dụng lần cuối cùng

- Phân tích dữ liệu

- Kiểm tra sự thay đổi cấu hình

- Kiểm tra hệ thống tập tin có bị mã độc

- Kiểm tra tập tin Internet history và các tập tin history khác

- Kiểm tra Registry và tiến trình

- Quan sát các tập tin, tiến trình lúc khởi động

- Phân tích log file

4.2.7 Xử lý sự cố

Văn phòng HĐND&UBND xã hoặc đơn vị tư vấn, triển khai tiến hành xử lý sự cố bao gồm các bước:

- Gỡ bỏ sự cố

- Xác định và gỡ bỏ các backdoors

- Phân tích và kiểm tra lỗ hỗng sau khi thực hiện các bản vá lỗi

- Khôi phục dữ liệu

- Thu thập các tập tin, hình ảnh, email, … bị xóa, thời gian bị xóa

- Tìm kiếm các tập tin không thể khôi phục

- Khôi phục các tập tin phù hợp

4.2.8 Tổng hợp báo cáo

Văn phòng HĐND&UBND xã hoặc đơn vị tư vấn, triển khai tiến hành tổng hợp kết quả phân tích và báo cáo kết quả với lãnh đạo, trong đó mô tả chi tiết các bước thực hiện, giải pháp xử lý sự cố, kết quả khắc phục hiện tại.

Văn phòng HĐND&UBND xã tiến hành tổng hợp toàn bộ các báo cáo phân tích có liên quan đến sự có để báo cáo với lãnh đạo đơn vị và Sở Thông tin và Truyền thông và Trung tâm giám sát ATTT Điện Biên. Họp phân tích nguyên nhân, rút kinh nghiệm trong hoạt động xử lý sự cố và đề xuất các biện pháp ứng dụng cho các sự cố tương tự.

4.2.9 Lưu hồ sơ

Toàn bộ các hồ sơ trong quá trình xử lý sự cố được lưu trữ phục vụ các hoạt động quản lý và theo dõi định kỳ.

5. Hồ sơ lưu trữ

STTT	Tên hồ sơ	Đơn vị lưu trữ
1	Thông báo sự cố	Văn phòng HĐND và UBND xã
2	Kế hoạch xử lý sự cố	

3	Hồ sơ xử lý sự cố	
4	Báo cáo phân tích kết quả điều tra xử lý sự cố	
5	Báo cáo thống kê hàng năm	

Phụ lục 05

DANH SÁCH PHẦN MỀM ĐƯỢC PHÉP CÀI ĐẶT TRÊN MÁY TRẠM

Stt	Tên phần mềm	Yêu cầu
1	7zip	Version 9 trở lên
2	Adobe AIR	Version 2.5 trở lên
3	Adobe Flash Builder	Không
4	Adobe Photoshop	Không
5	Adobe Premiere	Không
6	Adobe Reader	Version 9 trở lên
7	Bitdefender	Version 2012 trở lên
8	BKAV Pro	Bản mới nhất
9	C#	Không
10	C++	Không
11	Các Phần Mềm Subversion	Không
12	Chrome	Bản mới nhất
13	CPU-Z	Không
14	Dreamwear	Không
15	Dropbox	Version 3 trở lên
16	Esclipe	Không
17	Evernote	Version 5 trở lên
18	Filezilla Client	Version 3.9 trở lên
19	Firefox	Version 28 trở lên
20	Foxit Reader	Version 5 trở lên
21	Geany	Không
22	Gotiengviet	Không
23	Internet Download Manager	Version 6 trở lên
24	Itune	Không
25	Java	Version 7 trở lên
26	Kaspersky Antivirus	Version 2012 trở lên
27	Keepas	Version 2

28	Mantra	Không
29	Microsoft .NET Framework	Version 4.5 trở lên
30	Microsoft Security Essential	Bản mới nhất
31	Mindjet MindManager	Không
32	Ms Office	Version 2007 trở lên
33	MS Outlook	Version 2007 trở lên
34	MySQL Workbench	Không
35	Netbean	Không
36	Netscan	Không
37	Norton Antivirus	Version 2012 trở lên
38	Notepad++	Không
39	Open Office	Version 3 trở lên
40	Opera	Version 12 trở lên
41	Packet Tracer	Không
42	Phần mềm chụp màn hình Snagit	Version 8.0 trở lên
43	Phần mềm diệt virus Avast	Bản mới nhất
44	Phần mềm diệt virus Avg	Bản mới nhất
45	Phần mềm kế toán	Nhiều Version
46	Photoshop	Không
47	Pidgin	Không
48	PL/SQL Developer	Không
49	Power ISO	Version 5.8 trở lên
50	Putty	Không
51	Python	Version 2.6 trở lên
52	Reflector	Không
53	Remote Desktop	Không
54	RoyalTS	Không
55	Safari	Không
56	SCA BB Console	Không
57	SecureCRT	Không
58	Skype	Version 6 trở lên

59	Solarwind	Không
60	Sql Express	Không
61	SQL Navigator	Không
62	Sublime text	Không
63	SVN Client (TortoiseSVN)	Version 1.8 trở lên
64	TeamViewer	Version 9
65	Terminal Remote	Không
66	Thunderbirds	Version 24 trở lên
67	TOAD	Không
68	Ultra ISO	Không
69	Unikey	Version 4.0
70	Unity Web player	Không
72	VirtualBox	Version 5 trở lên
73	Visual Studio	Version 2010 trở lên
74	VLC Player	Version 2.2 trở lên
75	VMware vsphere	Version 4.1 trở lên
76	VMware workstation	Version 8 trở lên
77	WinPopcap	Không
78	Winrar	Version 4 trở lên
79	Winscp	Không
80	Wireshark	Không
81	xManager Enterprise	Version 4
82	xShell	Version 4