UBND TỈNH LÀO CAI **VĂN PHÒNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 03 /QĐ-VP	*Lào Cai, ngày 07 tháng 01 năm 2026*

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn Hệ thống thông tin của Văn phòng Ủy ban nhân dân tỉnh Lào Cai

CHÁNH VĂN PHÒNG ỦY BAN NHÂN DÂN TỈNH LÀO CAI

Căn cứ Luật tổ chức Chính quyền địa phương ngày 16/6/2025;

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

Căn cứ Luật An ninh mạng ngày 12/6/2018;

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

Căn cứ Thông tư số 31/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông về việc quy định hoạt động giám sát an toàn hệ thống thông tin;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông về việc Quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 10/2025/QĐ-UBND ngày 01/7/2025 của Ủy ban nhân dân tỉnh Lào Cai ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Văn phòng Ủy ban nhân dân tỉnh Lào Cai;

Xét đề nghị của Phòng Hành chính - Quản trị.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Quy chế bảo đảm an toàn Hệ thống thông tin của Văn phòng Ủy ban nhân dân tỉnh Lào Cai".

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

Điều 3. Trưởng các phòng, ban, đơn vị trực thuộc; công chức, viên chức và người lao động thuộc Văn phòng; các tổ chức, cá nhân liên quan căn cứ Quyết định thi hành./.

Nơi nhận:
- Như Điều 3;
- Chánh, Phó CVP UBND tỉnh;
- Lưu: VT, HCQT.

KT. CHÁNH VĂN PHÒNG
PHÓ CHÁNH VĂN PHÒNG

Nguyễn Thúc Mạnh

UBND TỈNH LÀO CAI
VĂN PHÒNG

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

QUY CHẾ BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN CỦA VĂN PHÒNG ỦY BAN NHÂN DÂN TỈNH

(Ban hành kèm theo Quyết định số:03/QĐ-VP ngày 07/01/2026 của Văn phòng Ủy ban nhân dân tỉnh Lào Cai)

Chương I
NHỮNG 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 Hệ thống thông tin do Văn phòng Ủy ban nhân dân tỉnh Lào Cai quản lý, vận hành.

2. Đối tượng áp dụng

a) Các phòng, ban, đơn vị sử dụng Hệ thống thông tin do Văn phòng Ủy ban nhân dân tỉnh Lào Cai quản lý và vận hành.

b) Cơ quan, tổ chức, cá nhân sử dụng Hệ thống thông tin do Văn phòng Ủy ban nhân dân tỉnh Lào Cai quản lý và vận hành.

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ phục vụ công tác quản lý, vận hành Hệ thống thông tin do Văn phòng Ủy ban nhân dân tỉnh Lào Cai quản lý.

Điều 2. Giải thích từ ngữ

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

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

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

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

4. *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 Hệ thống thông tin.

2. Nguyên tắc

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

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

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

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

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

Điều 4. Những hành vi nghiêm cấm

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

2. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập không dây của cá nhân vào mạng nội bộ; trên cùng một thiết bị thực hiện đồng thời truy cập vào mạng nội bộ và truy cập Internet bằng thiết bị kết nối Internet của cá nhân (modem quay số, USB 3G/4G, điện thoại di động, máy tính bảng, máy tính xách tay).

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

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) Văn phòng Ủy ban nhân dân tỉnh Lào Cai giao Phòng Hành chính - Quản trị là đầu mối liên hệ, phối hợp với Công an tỉnh Lào Cai, các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin phục vụ việc bảo đảm an toàn, an ninh mạng cho các Hệ thống thông tin của cơ quan. Thông tin liên hệ:

+ Số điện thoại: 0216.3852039

+ Email: vpubnd@laocai.gov.vn

b) Đơn vị có thẩm quyền quản lý về an toàn thông tin: Công an tỉnh Lào Cai.

- Người liên hệ/bộ phận: Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao;

+ Số điện thoại: 0692509858

+ Email: phonganm.cat@laocai.gov.vn.

2. Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền.

Điều 6. Bảo đảm nguồn nhân lực

1. Công chức, viên chức được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng.

2. Định kỳ hằng năm tham gia các lớp tập huấn, đào tạo về an toàn thông tin do Công an tỉnh, các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin tổ chức.

3. Trách nhiệm bảo đảm an toàn thông tin cho công chức, viên chức quản lý và vận hành hệ thống

a) Công chức, viên chức chuyên trách, bán chuyên trách công nghệ thông tin 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.

b) Công chức, viên chức chuyên trách, bán chuyên trách công nghệ thông tin phải tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin.

c) Các phòng chuyên môn, đơn vị và các tổ chức, cá nhân tham gia sử dụng các dịch vụ của hệ thống phải tuân thủ các quy định về bảo đảm an toàn, an ninh thông tin và chịu trách nhiệm đối với mọi hoạt động trên tài khoản truy cập của mình đã được cấp trên hệ thống.

4. Với người sử dụng

- Người sử dụng có trách nhiệm đảm bảo an toàn thông tin đối với từng vị trí công việc. Trước khi tham gia vào hệ thống phải được kiểm tra khả năng đáp ứng các yêu cầu về an toàn thông tin.

- Phải được thường xuyên tổ chức quán triệt các quy định về an toàn thông tin, nhằm nâng cao nhận thức về trách nhiệm đảm bảo an toàn thông tin.

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

- Có bản cam kết thực hiện quy chế bảo đảm an toàn thông tin đối với việc sử dụng, khai thác hệ thống thông tin.

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

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

b) Công chức quản trị công nghệ thông tin phải vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.

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

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

Điều 7. Thiết kế, xây dựng hệ thống thông tin

1. Xây dựng các tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin. Trong đó, phân công rõ trách nhiệm, nhiệm vụ của các đối tượng tham gia sử dụng, khai thác và vận hành hệ thống thông tin.

2. Xây dựng các tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin. Thường xuyên cập nhật, bổ sung các thành phần hệ thống thông tin khi thực hiện nâng cấp, mở rộng.

3. Khi lựa chọn các giải pháp công nghệ phải xây dựng các tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin. Tổ chức xin ý kiến các đơn vị quản lý về an toàn thông tin hoặc các chuyên gia có uy tín trong lĩnh vực an toàn thông tin.

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

5. Khi thiết kế xây dựng, nâng cấp, mở rộng hệ thống thông tin, chủ quản hệ thống thông tin phải đánh giá lại phương án bảo đảm an toàn thông tin trong hồ sơ thiết kế và gửi đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin thẩm định và phê duyệt cấp độ cho hệ thống thông tin trước khi trình cấp có thẩm quyền phê duyệt dự án.

6. Đánh giá, phân loại cấp độ an toàn thông tin của hệ thống thông tin

a) Chủ quản hệ thống thông tin có trách nhiệm tổ chức đánh giá, phân loại cấp độ an toàn thông tin của hệ thống thông tin theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống theo cấp độ (gọi tắt là Nghị định số 85/2016/NĐ-CP) và Thông tư số 24/2020/TT-BTTTT ngày 09/9/2020 của Bộ Thông tin và Truyền thông để áp dụng phương án bảo đảm an toàn thông tin phù hợp.

b) Hồ sơ đề xuất cấp độ bao gồm các tài liệu được quy định tại Điều 15, Nghị định số 85/2016/NĐ-CP, gửi đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin hoặc đơn vị chuyên trách về an toàn thông tin của Ủy ban nhân dân tỉnh thẩm định, trình cấp có thẩm quyền phê duyệt.

7. Trước khi đưa vào vận hành, khai thác hệ thống thông tin, Chủ quản hệ thống thông tin phải thực hiện kiểm thử hoặc vận hành thử trước khi đưa vào sử dụng. Kết quả kiểm thử, vận hành thử phải được lập thành văn bản và tuân thủ theo quy định tại Điều 10, Thông tư số 24/2020/TT-BTTTT ngày 09/9/2020 của Bộ trưởng 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.

Điều 8. Phát triển phần mềm thuê khoán

1. Có điều khoản hợp đồng và các cam kết đối với bên thuê khoán khi thực hiện các nội dung liên quan đến việc phát triển phần mềm thuê khoán. Trong đó phân công rõ nhiệm vụ, trách nhiệm của các bên có liên quan trong hợp đồng.

2. Các nhà phát triển cung cấp mã nguồn phần mềm, có biên bản bàn giao đi kèm.

3. Phần mềm thuê khoán phải được kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng.

4. Phần mềm thuê khoán phải được kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng.

Điều 9. Thử nghiệm và nghiệm thu hệ thống

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

2. Phải xây dựng kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống. Trong đó xác định rõ các nội dung thử nghiệm và nghiệm thu.

3. Phòng Hành chính - Quản trị có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống.

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

5. Có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản Hệ thống thông tin trước khi đưa vào sử dụng.

Điều 10. Bảo vệ bí mật nhà nước trong hoạt động ứng dụng công nghệ thông tin

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

a) Không được sử dụng máy tính nối mạng Internet để soạn thảo văn bản; chuyển giao, lưu trữ thông tin có nội dung thuộc bí mật nhà nước; cung cấp tin, tài liệu và đưa thông tin bí mật nhà nước trên Trang thông tin điện tử;

b) Không được in, sao chụp tài liệu bí mật nhà nước trên các thiết bị kết nối mạng internet;

c) Phải bố trí máy tính riêng, không kết nối mạng nội bộ và mạng Internet dùng để quản lý, soạn thảo các tài liệu mật của nhà nước theo quy định.

2. Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật, các phòng, đơn vị phải báo cáo cho người có thẩm quyền. Không được cho phép các tổ chức, cá nhân không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố.

3. Trước khi thanh lý các máy tính trong các cơ quan nhà nước, cán bộ chuyên trách công nghệ thông tin phải dùng các biện pháp kỹ thuật xóa bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

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

Điều 11. Quản lý an toàn mạng

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

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

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

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

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

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

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

2. 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.

Định kỳ cập nhật; sao lưu dự phòng các tập tin cấu hình hệ thống và khôi phục hệ thống sau khi xảy ra sự cố:

Sao lưu định kỳ thực hiện sao lưu hàng ngày (đối với cơ sở dữ liệu) và hàng tháng đối với tập tin cấu hình hệ thống.

Cập nhật: thực hiện khi có bản cập nhật mới của đơn vị cung cấp hệ thống.

3. Truy cập và quản lý cấu hình hệ thống

a) Công chức, viên chức và người lao động vận hành truy cập, khai thác thông tin tại Hệ thống thông tin 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) Tổ Công nghệ thông tin có quyền truy cập và quản lý cấu hình hệ thống thực hiện một số nhiệm vụ sau:

- Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống thông tin.

- Theo dõi và phát hiện các trường hợp truy cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, báo cáo cho cán bộ quản lý để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm.

- Tham mưu xây dựng quy trình quản lý an toàn người sử dụng đầu cuối.

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

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

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

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

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

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

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

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

2. Truy cập mạng của máy chủ

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

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

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

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

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

d) Phòng Hành chính - Quản trị có trách nhiệm quản lý truy cập và quản trị máy chủ và ứng dụng của hệ thống thông tin.

4. 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.

Sao lưu định kỳ thực hiện sao lưu hàng ngày (đối với cơ sở dữ liệu) và hàng tháng đối với tập tin cấu hình hệ thống.

5. Cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống máy chủ và ứng dụng: Đơn vị/bộ phận chuyên trách về công nghệ thông tin của đơn vị chịu trách nhiệm cài đặt phần mềm cho máy tính phục vụ công việc. Người dùng không được can thiệp vào các phần mềm đã cài đặt trên máy tính (thay đổi, gỡ bỏ…) khi chưa được sự đồng ý của bộ phận chuyên trách về công nghệ thông tin của đơn vị.

6. Kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống: Cấu hình tối ưu và tăng cường bảo mật cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác.

7. Các máy chủ trước khi đưa vào vận hành khai thác cần triển khai một số yêu cầu tối ưu và tăng cường bảo mật như:

a) Sử dụng hệ điều hành bảo đảm an toàn thông tin.

b) Loại bỏ hoặc tắt tất cả các dịch vụ không cần thiết.

c) Sử dụng các phiên bản phần mềm an toàn.

d) Kiểm soát truy cập và ghi nhận lại hoạt động (log) của tất cả các dịch vụ: Cấm tất cả các truy cập từ bên ngoài vào hệ thống, chỉ cấp quyền truy cập xác đáng cho các người dùng tin cậy.

e) Kiểm soát truy cập ở cấp người dùng cho mỗi dịch vụ.

Điều 13. Quản lý an toàn dữ liệu

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

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

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

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

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

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

a) Ban hành quy định về trao đổi thông tin tối thiểu gồm: Phân loại thông tin theo mức độ nhạy cảm; quyền và trách nhiệm của cá nhân khi tiếp cận thông tin; biện pháp đảm bảo tính toàn vẹn, bảo mật khi truyền nhận, xử lý, lưu trữ thông tin; chế độ bảo quản thông tin.

b) Các thông tin, tài liệu, dữ liệu nhạy cảm phải được mã hóa trước khi trao đổi, truyền nhận qua mạng máy tính.

c) Thực hiện các biện pháp quản lý, giám sát và kiểm soát chặt chẽ các trang/cổng thông tin điện tử cung cấp thông tin, dịch vụ, giao dịch trực tuyến cho các tổ chức, cá nhân bên ngoài.

d) Thực hiện biện pháp bảo vệ trang thiết bị, phần mềm phục vụ trao đổi thông tin nội bộ nhằm hạn chế việc xâm nhập, khai thác bất hợp pháp các thông tin nhạy cảm.

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

a) 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.

b) 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.

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

a) Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: Tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; Dữ liệu, thông tin nghiệp vụ và các thông tin, dữ liệu quan trọng khác trên hệ thống (nếu có).

b) 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.

c) 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 14. Quản lý an toàn thiết bị đầu cuối

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

1. 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.

Điều 15. Quản lý phòng, chống phần mềm độc hại

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

2. Khi gửi văn bản điện tử gửi qua hệ thống thư điện tử phải có định dạng theo Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước như: (.txt), (.doc), (.odt), (.pdf) và các định dạng khác theo quy định, không được gửi các file thực thi (.com), (.bat), (.exe) ….

3.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.

4. 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.

5. 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.

6. 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.

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

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

1. Triển khai hệ thống giám sát trung tâm phải đáp ứng yêu cầu tại khoản 1, Điều 5 Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông về Quy định hoạt động giám sát an toàn hệ thống thông tin.

2. Thông tin giám sát và danh mục các đối tượng giám sát phải đáp ứng yêu cầu tại khoản 2, Điều 5, Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông. Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát.

3. Thực thi nhiệm vụ giám sát theo quy định tại khoản 3, Điều 5, Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông.

4. Định kỳ hằng năm tổ chức nâng cao năng lực hoạt động giám sát theo quy định tại Điều 9, Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông.

5. Chủ quản hệ thống thông tin có trách nhiệm giám sát an toàn thông tin theo quy định tại Điều 14, Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông.

Điều 17. Quản lý điểm yếu an toàn thông tin

1. Đơn vị hoặc Bộ phận chuyên 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 giảm 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.

d) Có trách nhiệm phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin đối với các điểm yếu khi cần thiết.

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

3. Hoạt động đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thực hiện theo quy định tại điểm c, khoản 2, Điều 20, Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ và Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông về việc quy định chi tiết và hướng dẫn một số điều của nghị định số 85/2016/NĐ-CP.

Điều 18. Quản lý sự cố an toàn thông tin

1. Phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; 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.

2. 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 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ về việc Ban hành Quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng Quốc gia.

3. Xây dựng và triển khai kế hoạch ứng phó sự cố an toàn thông tin theo quy định tại Điều 16, Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ về việc Ban hành Quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng Quốc gia.

4. Quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về an toàn thông tin; Hỗ trợ, phối hợp và hướng dẫn các cơ quan

khắc phục sự cố mất an toàn thông tin; 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 an toàn thông tin; 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.

5. 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.

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) Máy tính, thiết bị đầu cuối phải được xử lý điểm yếu an toàn thông tin, cấu hình 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. Quy định, quy trình về Kết thúc vận hành, khai thác, thanh lý, hủy bỏ bao gồm các nội dung sau:

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

b) Trước khi tiến hành thanh lý/loại bỏ thiết bị công nghệ thông tin cũ, phải áp dụng các biện pháp kỹ thuật xóa bỏ hoàn toàn dữ liệu người dùng đã tạo ra, đảm bảo không thể phục hồi.

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

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

Điều 20. Nội dung, hình thức kiểm tra, đánh giá

1. Mục đích và phạm vi áp dụng:

Nhằm nhận diện, đánh giá, xử lý và giám sát các rủi ro có thể ảnh hưởng đến an toàn thông tin của hệ thống mạng nội bộ (LAN) và các hệ thống thông tin có liên quan của cơ quan.

2. Nội dung kiểm tra, đánh giá

a) Kiểm tra việc thực hiện các nội dung tại quy chế này; kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ.

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

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

d) Kiểm tra, đánh giá khác do chủ quản hệ thống thông tin quy định và theo quy định của hệ thống an toàn thông tin.

3. Hình thức kiểm tra, đánh giá

a) Kiểm tra, đánh giá định kỳ theo kế hoạch của chủ quản hệ thống thông tin, theo kế hoạch của Văn phòng Ủy ban nhân dân tỉnh Lào Cai và đơn vị chuyên trách về an toàn thông tin của tỉnh.

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

4. Cấp có thẩm quyền yêu cầu kiểm tra, đánh giá

a) Đơn vị chuyên trách an toàn thông tin.

b) Ủy ban nhân dân tỉnh hoặc Công an tỉnh Lào Cai.

c) Văn phòng Ủy ban nhân dân tỉnh Lào Cai giao nhiệm vụ kiểm tra về an toàn thông tin cho Phòng Hành chính - Quản trị thực hiện.

5. Đơn vị chủ trì kiểm tra, đánh giá là đơn vị được cấp có thẩm quyền giao nhiệm vụ hoặc được lựa chọn để thực hiện nhiệm vụ kiểm tra, đánh giá.

6. Đối tượng kiểm tra, đánh giá là chủ quản hệ thống thông tin hoặc đơn vị vận hành hệ thống thông tin và các hệ thống thông tin có liên quan.

Điều 21. Kế hoạch kiểm tra hằng năm

1. Phòng Hành chính - Quản trị chủ trì, phối hợp với các đơn vị liên quan tiến hành kiểm tra công tác đảm bảo an toàn thông tin của Văn phòng theo Kế hoạch công tác hằng năm.

2. Tiến hành kiểm tra đột xuất các phòng, đơn vị trực thuộc khi có dấu hiệu vi phạm an toàn đối với các hệ thống thông tin của Văn phòng.

Chương V
BÁO CÁO, CHIA SẺ THÔNG TIN

Điều 22. Chế độ báo cáo

1. Báo cáo định kỳ

a) Báo cáo an toàn thông tin định kỳ hằng năm gồm các nội dung quy định tại Điều 14, Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông.

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 số 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.

Điều 23. Chia sẻ thông tin

Việc chia sẻ dữ liệu số của các hệ thống thông tin với các cơ quan nhà nước được thực hiện theo quy định tại Nghị định số 47/2020/NĐ-CP ngày 09/4/2020 của Chính phủ về việc quản lý, kết nối và chia sẻ dữ liệu của cơ quan nhà nước.

Chương VI
TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 24. Đơn vị vận hành

1. Thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo quy định tại Điều 22, Nghị định số 85/2016/NĐ-CP, tại Quy chế này và các nhiệm vụ do chủ quản hệ thống thông tin phân công.

2. Chỉ đạo các phòng, đơn vị trực thuộc thực hiện quản lý ứng dụng; quản lý dữ liệu; 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.

3. Lập hồ sơ đề xuất cấp độ, gửi về Đơn vị hoặc Bộ phận chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin thẩm định *(theo quy định tại Nghị định 85/2016/NĐ-CP).*

Điều 25. Trách nhiệm của Đơn vị/Bộ phận chuyên trách, bán chuyên trách về ATTT

1. Phòng Hành chính - Quản trị; các đơn vị trực thuộc thực thi nhiệm vụ bảo đảm an toàn thông tin và ứng cứu sự cố an toàn thông tin mạng theo các quy định tại Quy chế này và hướng dẫn các công chức, viên chức và người lao động của Văn phòng Ủy ban nhân dân tỉnh Lào Cai triển khai đảm bảo an toàn, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin tại đơn vị mình.

2. Thẩm định hồ sơ cấp độ 1, 2 *(quy định tại khoản 1, Điều 12 của Nghị định số 85/2016/NĐ-CP)* và gửi hồ sơ cấp độ về Công an tỉnh Lào Cai để phê duyệt hồ sơ cấp độ.

Điều 26. Trách nhiệm của đơn vị cung cấp dịch vụ

1. Đơn vị cung cấp dịch vụ có trách nhiệm bảo đảm cung cấp đầy đủ các thành phần, chức năng; Thiết kế, thiết lập hệ thống đáp ứng các yêu cầu kỹ thuật các cấp độ theo tiêu chuẩn quy định.

2. Quản lý, vận hành, bảo đảm an toàn thông tin cho các thành phần hệ thống thuộc phạm vi quản lý của mình tuân thủ các quy định tại Quy chế này.

3. Lập hồ sơ cấp độ của hệ thống thông tin, gửi về đơn vị vận hành hệ thống để chuyển đến đơn vị, các cấp có thẩm quyền thẩm định, phê duyệt hệ thống.

Điều 27. Trách nhiệm của đơn vị, tổ chức, cá nhân sử dụng hệ thống

Sử dụng hệ thống thông tin đảm bảo an toàn thông tin theo Quy chế này.

Điều 28. Bảo đảm an ninh mạng

Thực hiện theo Điều 12, Điều 13, Điều 14 của Quyết định số 1512/QĐ- BTTTT ngày 05/10/2021 của Bộ trưởng Bộ Thông tin và Truyền thông về việc ban hành Quy chế bảo đảm an toàn thông tin mạng và an ninh mạng; các quy định khác có liên quan.

Điều 29. Trách nhiệm của bộ phận phụ trách công tác đảm bảo an toàn thông tin

1. Thành lập hoặc chỉ định bộ phận phụ trách công tác đảm bảo an toàn thông tin của Văn phòng Ủy ban nhân dân tỉnh Lào Cai.

2. Phân định vai trò, trách nhiệm, cơ chế phối hợp của bộ phận với các tổ chức, cá nhân trong và ngoài Văn phòng Ủy ban nhân dân tỉnh Lào Cai.

Điều 30. Phối hợp với những cơ quan/tổ chức có thẩm quyền

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

2. Có 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.

3. Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền.

Chương VI
TỔ CHỨC THỰC HIỆN

Điều 31. Tổ chức triển khai Quy chế

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

2. Trong quá trình thực hiện nếu có vấn đề phát sinh, vướng mắc, các đơn vị liên quan phản ánh kịp thời về Bộ phận chuyên trách để xem xét, bổ sung, sửa đổi.

Điều 32. Xây dựng, rà soát, cập nhật, bổ sung Quy chế

1. Định kỳ 03 năm hoặc khi có thay đổi chính sách an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung. Quy chế Bảo đảm an toàn, an ninh mạng đối với Hệ thống thông tin này được Văn phòng Ủy ban nhân dân tỉnh Lào Cai thông qua trước khi công bố và được công bố trước khi áp dụng.

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

3. Quy chế này được phổ biến, tuyên truyền đến toàn bộ công chức, viên chức và người lao động của Văn phòng Ủy ban nhân dân tỉnh Lào Cai và các tổ chức, cá nhân có liên quan.

Điều 33. Bộ phận chuyên trách về an toàn thông tin

1. Giao Bộ phận công nghệ thông tin, chuyển đổi số thuộc Phòng Hành chính - Quản trị thực hiện các nhiệm vụ về bảo đảm an toàn thông tin cho hệ thống.

2. Bộ phận công nghệ thông tin, chuyển đổi số thuộc Phòng Hành chính - Quản trị chủ trì, phối hợp với các cơ quan, đơn vị có liên quan nghiên cứu và tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hằng năm hoặc theo chỉ đạo của Lãnh đạo Văn phòng Ủy ban nhân dân tỉnh Lào Cai.

3. Triển khai các phương án đảm bảo an toàn thông tin tại cơ quan.

Điều 34. Các phòng chuyên môn, đơn vị trực thuộc Văn phòng

1. Căn cứ Quy chế này, Lãnh đạo Văn phòng, lãnh đạo các phòng, ban chuyên môn trực thuộc có trách nhiệm tổ chức triển khai thực hiện Quy chế này trong phạm vi quản lý của mình.

2. Phòng Hành chính - Quản trị có trách nhiệm theo dõi, đôn đốc, kiểm tra, đánh giá việc thực hiện Quy chế, báo cáo Lãnh đạo Văn phòng theo định kỳ hằng năm hoặc đột xuất theo yêu cầu của Ủy ban nhân dân tỉnh và cơ quan có thẩm quyền của tỉnh.

3. Trong quá trình thực hiện Quy chế, nếu có vấn đề vướng mắc, phát sinh, các phòng chuyên môn, đơn vị trực thuộc phản ánh kịp thời về Văn phòng Ủy ban nhân dân tỉnh Lào Cai (qua Phòng Hành chính - Quản trị) để tổng hợp xem xét điều chỉnh, bổ sung./.

BỘ QUY TRÌNH AN TOÀN THÔNG TIN CẤP ĐỘ 2

(Áp dụng tại: Quyết định số: 03/QĐ-VP ngày 07/01/2025 về việc ban hành Quy chế bảo đảm an toàn Hệ thống thông tin của Văn Ủy ban nhân dân tỉnh Lào Cai)

Quy trình 1: Vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên và quản trị hệ thống sau khi cán bộ thôi việc

1. Mục đích

Đảm bảo thu hồi toàn bộ quyền truy cập và phương tiện làm việc của cán bộ ngay khi chấm dứt quan hệ lao động để phòng ngừa truy cập trái phép.

2. Phạm vi áp dụng

Áp dụng cho toàn bộ hệ thống thông tin, mạng, ứng dụng, email, SSO và quyền ra/vào tại đơn vị

3. Định nghĩa, thuật ngữ

• Tài khoản hệ thống: tài khoản AD/SSO, email, ứng dụng, VPN.

• Quyền truy cập vật lý: thẻ ra/vào, chìa khóa, thiết bị được cấp.

4. Nội dung quy trình (theo bước)

Bước 1: Tiếp nhận quyết định/Thông báo nghỉ việc từ Phòng Hành chính – Quản trị (trong 01 ngày).

Bước 2: Khóa tài khoản SSO/AD/email/VPN và thu hồi quyền truy cập trên các ứng dụng nghiệp vụ (trong 04 giờ làm việc kể từ khi nhận thông báo).

Bước 3: Thu hồi phương tiện vật lý: thẻ, chìa khóa, laptop/điện thoại, USB token, sim OTP.

Bước 4: Bàn giao dữ liệu công việc cho người kế nhiệm/đơn vị quản lý; chuyển quyền sở hữu tài liệu số.

Bước 5: Lập Biên bản thu hồi (Mẫu 01/ATTT) và cập nhật nhật ký hệ thống thời điểm khóa tài khoản.

Bước 6: Rà soát danh sách người dùng vào cuối mỗi quý để bảo đảm không còn tài khoản của người đã nghỉ.

5. Trách nhiệm thực hiện

• Phòng Hành chính - Quản trị: thông báo kịp thời danh sách nghỉ việc/điều chuyển.

• Bộ phận CNTT thuộc Phòng Hành chính - Quản trị: khóa tài khoản, thu hồi quyền, đối soát nhật ký.

• Phòng Hành chính – Quản trị: thu hồi thẻ/thiết bị vật lý.

• Quản lý trực tiếp: tổ chức bàn giao dữ liệu và công việc.

6. Biểu mẫu/Hồ sơ liên quan

• Mẫu 01/ATTT – Biên bản thu hồi tài khoản & thiết bị

• Nhật ký hệ thống (log)

Quy trình 2: Thử nghiệm và nghiệm thu hệ thống

1. Mục đích

Bảo đảm hệ thống sau triển khai/cập nhật đáp ứng yêu cầu nghiệp vụ và an toàn thông tin trước khi vận hành chính thức.

2. Phạm vi áp dụng

Áp dụng cho hệ thống thông tin cấp độ 2 trở lên (hạ tầng, phần mềm, CSDL, cấu hình bảo mật).

3. Định nghĩa, thuật ngữ

• Thử nghiệm: kiểm tra chức năng/hiệu năng/ATTT theo kế hoạch.

• Nghiệm thu: đánh giá và xác nhận chính thức trước khi vận hành.

4. Nội dung quy trình (theo bước)

Bước 1: Lập Kế hoạch thử nghiệm (phạm vi, tiêu chí, kịch bản, dữ liệu test) và trình phê duyệt.

Bước 2: Thực hiện thử nghiệm chức năng - đối chiếu yêu cầu nghiệp vụ.

Bước 3: Thử nghiệm hiệu năng và ổn định - đo tải, thời gian đáp ứng.

Bước 4: Kiểm tra ATTT - rà soát phân quyền, backup/restore, quét lỗ hổng.

Bước 5: Tổng hợp lỗi, nhà thầu khắc phục; tái kiểm tra.

Bước 6: Tổ chức nghiệm thu bởi Hội đồng; ký Biên bản nghiệm thu (Mẫu 03/ATTT).

Bước 7: Lưu trữ hồ sơ: KH thử nghiệm, BB thử nghiệm (Mẫu 02/ATTT), BB nghiệm thu.

5. Trách nhiệm thực hiện

• Bộ phận CNTT thuộc Phòng Hành chính - Quản trị: chủ trì lập kế hoạch và tổ chức thử nghiệm.

• Đơn vị triển khai/nhà thầu: cung cấp tài liệu, khắc phục lỗi.

• Đơn vị nghiệp vụ: tham gia test chấp nhận người dùng (UAT).

• Lãnh đạo: phê duyệt kế hoạch, quyết định nghiệm thu.

6. Biểu mẫu/Hồ sơ liên quan

• Mẫu 02/ATTT – Biên bản thử nghiệm

• Mẫu 03/ATTT – Biên bản nghiệm thu

• Báo cáo quét lỗ hổng/kiểm thử

Quy trình 3: Quản lý an toàn mạng

1. Mục đích

Thiết lập, vận hành và giám sát an ninh mạng để phòng ngừa, phát hiện và ứng phó rủi ro tấn công, rò rỉ dữ liệu.

2. Phạm vi áp dụng

Áp dụng cho toàn bộ hạ tầng mạng (LAN/WAN/Wi-Fi/DMZ), kết nối Internet, thiết bị bảo mật tại đơn vị.

3. Định nghĩa, thuật ngữ

• Vùng mạng: LAN nội bộ, DMZ, vùng quản trị.

• Thiết bị an ninh: tường lửa, IDS/IPS, WAF, VPN.

4. Nội dung quy trình (theo bước)

Bước 1: Kiểm kê, phân loại tài sản mạng; lập sơ đồ mạng được phê duyệt.

Bước 2: Phân vùng mạng theo mức độ tin cậy (LAN/DMZ/quản trị); áp dụng nguyên tắc tối thiểu đặc quyền.

Bước 3: Cấu hình tường lửa – chính sách allowlist theo dịch vụ; bật NAT, chống giả mạo (anti-spoofing).

Bước 4: Triển khai và tinh chỉnh IDS/IPS/WAF; thiết lập cảnh báo bất thường.

Bước 5: Bật ghi log tập trung; đồng bộ thời gian (NTP); lưu giữ log tối thiểu 06–12 tháng.

Bước 6: Quản lý truy cập từ xa qua VPN bảo mật (MFA, certificate); vô hiệu hóa truy cập trái phép.

Bước 7: Định kỳ cập nhật bản vá/firmware, sao lưu cấu hình; kiểm tra tuân thủ và đánh giá an toàn tối thiểu 01 lần/năm.

5. Trách nhiệm thực hiện

• Bộ phận CNTT: vận hành, giám sát, sao lưu cấu hình.

• Lãnh đạo: phê duyệt sơ đồ mạng, chính sách an ninh.

• Nhà thầu/nhà cung cấp: hỗ trợ kỹ thuật, cập nhật bảo trì.

6. Biểu mẫu/Hồ sơ liên quan

• Nhật ký thiết bị mạng

• Kế hoạch/biên bản kiểm tra an toàn mạng

Quy trình 4: Quản lý an toàn máy chủ và ứng dụng

1. Mục đích

Bảo đảm an toàn cho máy chủ vật lý/ảo, hệ điều hành, phần mềm trung gian và ứng dụng nghiệp vụ.

2. Phạm vi áp dụng

Áp dụng cho máy chủ tại DC/đám mây, hệ điều hành Windows/Linux, DBMS, middleware và ứng dụng web/dịch vụ.

3. Định nghĩa, thuật ngữ

• Chuẩn cấu hình an toàn (baseline) và tiêu chuẩn hardening hệ điều hành/DBMS.

• Nguyên tắc phân quyền tối thiểu đối với tài khoản quản trị.

4. Nội dung quy trình (theo bước)

Bước 1: Thiết lập baseline/hardening: tắt dịch vụ không cần thiết, cấu hình tường lửa nội bộ, nhật ký sự kiện.

Bước 2: Quản lý tài khoản đặc quyền (PAM): đặt tên quy ước, MFA, đổi mật khẩu định kỳ; không dùng tài khoản mặc định.

Bước 3: Cập nhật bản vá OS/phần mềm theo lịch; kiểm thử trước khi áp dụng trên môi trường sản xuất.

Bước 4: Cài và cập nhật giải pháp chống mã độc/EDR; quét định kỳ theo lịch.

Bước 5: Sao lưu hệ thống và cơ sở dữ liệu theo chính sách; diễn tập khôi phục tối thiểu 01 lần/năm.

Bước 6: Kiểm thử bảo mật ứng dụng trước khi triển khai (quét lỗ hổng, kiểm tra cấu hình); đánh giá thay đổi (change review).

Bước 7: Giám sát log máy chủ/ứng dụng; cảnh báo truy cập bất thường; lưu trữ log theo quy định.

5. Trách nhiệm thực hiện

• Quản trị hệ thống: thực hiện hardening, vá lỗi, sao lưu.

• Quản trị ứng dụng/DBA: quản lý cấu hình, phân quyền dữ liệu.

• Bộ phận CNTT: giám sát, tổng hợp báo cáo tuân thủ.

6. Biểu mẫu/Hồ sơ liên quan

• Checklist hardening

• Kế hoạch vá lỗi

• Biên bản diễn tập khôi phục

Quy trình 5: Quản lý an toàn dữ liệu

1. Mục đích

Đảm bảo tính bí mật, toàn vẹn, sẵn sàng của dữ liệu trong toàn bộ vòng đời.

2. Phạm vi áp dụng

Áp dụng cho dữ liệu vận hành, sao lưu, nhật ký, dữ liệu nhạy cảm/cá nhân trong các hệ thống cấp độ 2.

3. Định nghĩa, thuật ngữ

• Phân loại dữ liệu theo độ nhạy (Công khai/Nội bộ/Mật/NN).

• Mã hóa khi lưu trữ (at-rest) và truyền tải (in-transit) đối với dữ liệu nhạy cảm.

4. Nội dung quy trình (theo bước)

Bước 1: Phân loại và gán nhãn dữ liệu; lập danh mục tập dữ liệu và chủ sở hữu dữ liệu.

Bước 2: Thiết lập quyền truy cập dựa trên vai trò (RBAC); định kỳ rà soát quyền.

Bước 3: Sao lưu: toàn bộ 01 lần/tuần và gia tăng hằng ngày; kiểm tra phục hồi mẫu.

Bước 4: Áp dụng mã hóa/che giấu dữ liệu (masking) cho môi trường test/dev.

Bước 5: Quy định truyền/nhận dữ liệu ra ngoài (VPN, SFTP, ký số); kiểm soát thiết bị ngoại vi.

Bước 6: Quy định thời hạn lưu trữ và hủy tiêu hủy an toàn (ghi biên bản hủy).

Bước 7: Theo dõi truy cập dữ liệu quan trọng; audit định kỳ và đột xuất.

5. Trách nhiệm thực hiện

• Chủ sở hữu dữ liệu: phê duyệt truy cập, định nghĩa mức nhạy.

• DBA/quản trị hệ thống: vận hành sao lưu, mã hóa, phục hồi.

• Bộ phận CNTT thuộc Phòng Thông tin – Dân nguyện: kiểm tra tuân thủ, báo cáo định kỳ.

6. Biểu mẫu/Hồ sơ liên quan

• Chính sách phân loại dữ liệu

• Kế hoạch sao lưu/khôi phục

• Biên bản tiêu hủy dữ liệu

Quy trình 6: Quản lý sự cố an toàn thông tin

1. Mục đích

Thiết lập quy trình phát hiện, phân loại, ứng phó và báo cáo sự cố ATTT kịp thời, giảm thiểu tác động.

2. Phạm vi áp dụng

Áp dụng cho tất cả người dùng, hệ thống, dịch vụ CNTT.

3. Định nghĩa, thuật ngữ

• CSIRT: Đội ứng cứu sự cố cấp đơn vị; kênh liên hệ 24/7.

• Phân loại mức độ sự cố: cao/trung bình/thấp.

4. Nội dung quy trình (theo bước)

Bước 1: Phát hiện và ghi nhận: người dùng hoặc hệ thống cảnh báo; tạo vé/ticket sự cố.

Bước 2: Phân loại và kích hoạt CSIRT; thông báo các bên liên quan.

Bước 3: Khoanh vùng/kiềm chế: cô lập thiết bị/tài khoản; chặn luồng tấn công.

Bước 4: Xử lý/loại bỏ nguyên nhân và khôi phục dịch vụ an toàn.

Bước 5: Thu thập bằng chứng, cập nhật nhật ký; đánh giá tác động.

Bước 6: Báo cáo sự cố theo thẩm quyền; nếu nghiêm trọng, báo cáo cơ quan chuyên trách theo quy định.

Bước 7: Rút kinh nghiệm sau sự cố; cập nhật quy trình/biện pháp phòng ngừa.

5. Trách nhiệm thực hiện

• CSIRT: chỉ huy ứng phó, phân công nhiệm vụ.

• Bộ phận CNTT thuộc Phòng Thông tin – Dân nguyện: thực hiện kỹ thuật, ghi nhận bằng chứng.

• Đơn vị nghiệp vụ: phối hợp cung cấp thông tin, hỗ trợ khôi phục.

• Lãnh đạo: phê duyệt thông tin công bố và báo cáo.

6. Biểu mẫu/Hồ sơ liên quan

• Biểu mẫu báo cáo sự cố

• Nhật ký sự cố

• Kế hoạch truyền thông sự cố

Quy trình 7: Quản lý an toàn người sử dụng đầu cuối

1. Mục đích

Nâng cao an toàn từ phía người dùng, giảm rủi ro do hành vi và thiết bị đầu cuối.

2. Phạm vi áp dụng

Áp dụng cho cán bộ/nhân viên, cộng tác viên, tài khoản khách và thiết bị đầu cuối được phép kết nối vào hệ thống.

3. Định nghĩa, thuật ngữ

• Người dùng cuối: người sử dụng dịch vụ, thiết bị CNTT của đơn vị.

• RBAC/MFA: phân quyền theo vai trò và xác thực đa yếu tố.

4. Nội dung quy trình (theo bước)

Bước 1: Tiếp nhận yêu cầu và tạo/cấp quyền tài khoản theo phân quyền đã phê duyệt.

Bước 2: Trang bị/đăng ký thiết bị: cài đặt EDR/antivirus, cấu hình mã PIN/MFA.

Bước 3: Tập huấn định kỳ về ATTT, chính sách sử dụng; ký cam kết tuân thủ.

Bước 4: Thực thi chính sách mật khẩu mạnh và đổi định kỳ; bật MFA cho dịch vụ quan trọng.

Bước 5: Kiểm soát cài đặt phần mềm: chỉ cài từ kho được phép; chặn USB ngoại vi nếu không cần thiết.

Bước 6: Giám sát và nhắc nhở vi phạm; xử lý kỷ luật theo quy định khi tái phạm.

Bước 7: Thu hồi tài khoản/quyền/thiết bị khi thôi nhiệm hoặc điều chuyển (liên thông với Quy trình 1).

5. Trách nhiệm thực hiện

• Bộ phận CNTT/helpdesk: tạo tài khoản, hỗ trợ kỹ thuật, giám sát thiết bị.

• Quản lý trực tiếp: phê duyệt quyền, theo dõi tuân thủ nhân viên.

• Người dùng: chịu trách nhiệm bảo mật tài khoản/thiết bị của mình.

6. Biểu mẫu/Hồ sơ liên quan

• Biểu mẫu đề nghị cấp quyền

• Danh mục phần mềm cho phép

• Biên bản nhắc nhở/vi phạm.

PHỤ LỤC I – Biên bản thu hồi tài khoản & thiết bị

Mẫu 01/ATTT – Biên bản thu hồi tài khoản & thiết bị

CƠ QUAN/ĐƠN VỊ: …….

Số: ……/BB-TH

Hôm nay, ngày … tháng … năm …, tại ……, chúng tôi gồm:

- Đại diện đơn vị quản lý tài khoản, thiết bị CNTT: ……

- Đại diện đơn vị phụ trách CNTT: ……

- Người bàn giao (cán bộ thôi việc): ……

1. Tài khoản đã thu hồi: ……

2. Thiết bị đã thu hồi: ……

Các bên thống nhất ký xác nhận.

PHỤ LỤC II – Biên bản thử nghiệm hệ thống

Mẫu 02/ATTT – Biên bản thử nghiệm hệ thống

CƠ QUAN/ĐƠN VỊ: …….

Số: ……/BB-TN

Ngày … tháng … năm …, tiến hành thử nghiệm hệ thống ……

Hội đồng thử nghiệm gồm: …….

- Thử nghiệm chức năng: ……

- Thử nghiệm hiệu năng: ……

- Thử nghiệm ATTT (quét lỗ hổng, phân quyền, backup/restore): ……

Kết quả/Khuyến nghị: ……

PHỤ LỤC III – Biên bản thử nghiệm hệ thống

Mẫu 03/ATTT – Biên bản nghiệm thu hệ thống

CƠ QUAN/ĐƠN VỊ: …….

Số: ……/BB-NT

Hội đồng nghiệm thu gồm: ……...

Tiến hành nghiệm thu hệ thống: ……

Căn cứ: KH thử nghiệm, BB thử nghiệm, báo cáo khắc phục.

Kết quả: hệ thống đáp ứng/không đáp ứng yêu cầu; chấp nhận/không chấp nhận đưa vào vận hành.