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

QUY CHẾ
Bảo đảm an toàn thông tin mạng nội bộ tại UBND xã Lộc Bình
(Kèm theo Quyết định số 1232/QĐ-UBND ngày 28/9/2026 của UBND xã Lộc Bình)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Quan điểm, phạm vi áp dụng

1. Quan điểm

An toàn thông tin, an ninh mạng là vấn đề quan trọng và cấp thiết của mọi cơ quan, đơn vị. Việc bảo đảm an toàn thông tin, an ninh mạng không chỉ là nhiệm vụ riêng của bộ phận an toàn thông tin mà còn là trách nhiệm của toàn bộ các đơn vị và cán bộ, công chức, viên chức trực thuộc UBND xã.

2. Phạm vi áp dụng

Quy chế này quy định về công tác quản lý và bảo đảm an toàn thông tin, an ninh mạng, quyền hạn, trách nhiệm của các cơ quan, đơn vị, cá nhân trong quản lý và bảo đảm an toàn thông tin, an ninh mạng trong UBND xã.

Điều 2. Đối tượng áp dụng

a) Các cơ quan, đơn vị thuộc UBND xã và cán bộ, công chức, viên chức, người lao động thuộc UBND xã.

b) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin và an toàn thông tin mạng cho Văn phòng HĐND và UBND xã.

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ quản lý, vận hành, duy trì, phát triển và bảo đảm an toàn thông tin mạng phục vụ hoạt động cho các Hệ thống thông tin do Văn phòng HĐND và UBND xã quản lý.

Điều 3. 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. *Chủ quản hệ thống thông tin* là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin.

5. *Sự cố an toàn thông tin mạng* là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

6. *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.

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

8. *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.

9. Các thuật ngữ, tên công nghệ phổ biến được nêu trong Quy chế này:

SSL (Secure Sockets Layer): Giao thức mã hóa kênh truyền dữ liệu kết nối an toàn giữa máy chủ web (host) và trình duyệt web (client) web.

TLS (Transport Layer Security): Giao thức Bảo mật tầng vận chuyển, giao thức mật mã cung cấp bảo mật đầu cuối cho dữ liệu được gửi giữa các ứng dụng qua Internet.

SSH (Secure Shell): đây là một giao thức hỗ trợ các nhà quản trị mạng truy cập vào máy chủ từ xa thông qua mạng internet không bảo mật.

VPN (*Virtual Private Network*): mạng riêng ảo, là một công nghệ mạng giúp tạo kết nối mạng an toàn khi tham gia vào mạng công cộng như Internet hoặc mạng riêng do một nhà cung cấp dịch vụ sở hữu, để cho phép người dùng từ xa kết nối an toàn đến mạng riêng của cơ quan mình.

LAN (*Local Area Network*): mạng cục bộ, mạng nội bộ kết nối máy tính, thiết bị tại mỗi phòng ban, cơ quan, đơn vị, có thể sử dụng kết nối giao thức TCP/IP (Transmission Control Protocol/Internet Protocol: giao thức điều khiển truyền nhận/ Giao thức liên mạng, một bộ các giao thức truyền thông được sử dụng để kết nối các thiết bị mạng với nhau trên internet. TCP/IP cũng có thể được sử dụng như một giao thức truyền thông trong mạng máy tính riêng (mạng nội bộ) có dây hoặc không dây).

Điều 4. Mục tiêu, nguyên tắc bảo đảm an toàn thông tin mạng

1. Mục tiêu

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 cho các Hệ thống thông tin tại UBND xã.

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 các Hệ thống thông tin tại UBND xã 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.

d) Các phòng, đơn vị sự nghiệp trực thuộc UBND xã có trách nhiệm bảo đảm an toàn, an ninh thông tin mạng của đơn vị mình; bố trí nhân sự chịu trách nhiệm bảo đảm an toàn, an ninh thông tin mạng; xác định rõ quyền hạn, trách nhiệm từng bộ phận, cá nhân trong đơn vị đối với công tác bảo đảm an toàn, an ninh thông tin mạng.

Điều 5. Những hành vi nghiêm cấm

1. Các hành vi bị nghiêm cấm quy định tại Điều 7 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 mạng không dây của cá nhân vào mạng nội bộ.

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

4. Tạo ra, cài đặt, phát tán phần mềm độc hại.

5. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin; ngăn chặn việc truy nhập đến thông tin của cơ quan, cá nhân khác trên môi trường mạng, trừ trường hợp pháp luật cho phép.

6. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

7. Các hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

Điều 6. 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 HĐND và UBND xã là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin phục vụ việc bảo đảm an toàn, an ninh mạng cho các Hệ thống thông tin do các đơn vị trực thuộc UBND xã vận hành, quản lý; tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin của các Hệ thống thông tin thuộc UBND xã; phối hợp với các cơ

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

b) Các đơn vị cử đầu mối tiếp nhận và xử lý các sự cố về an toàn thông tin của các hệ thống thông tin do các đơn vị trực tiếp vận hành, khai thác.

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

Điều 7. Bảo vệ bí mật nhà nước trong ứng dụng công nghệ thông tin

1. Quy định về soạn thảo, in ấn, phát hành và sao chụp tài liệu mật thực hiện theo quy định tại các khoản 5, 6, 9 Điều 5 Luật Bảo vệ bí mật nhà nước và quy định khác có liên quan.

2. Khi máy tính dùng để soạn thảo văn bản mật có sự cố thực hiện theo quy định tại Điều 9 Quyết định số 57/2026/QĐ-UBND ngày 25/8/2026 của UBND tỉnh Lạng Sơn.

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

Điều 8. Bảo đảm nguồn nhân lực

1. Khi xây dựng đề án vị trí việc làm, đơn vị phải bố trí 01 vị trí việc làm công nghệ thông tin.

2. Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng, theo đề án vị trí việc làm được duyệt.

3. Trong quá trình làm việc

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

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

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

d) Thường xuyên tổ chức, phổ biến các quy định về đảm bảo an toàn thông tin, nhằm nâng cao nhận thức về trách nhiệm đảm bảo an toàn thông tin cho tổ chức, cá nhân sử dụng hệ thống thông tin do đơn vị quản lý.

4. Chấm dứt thay đổi công việc

Khi công chức, viên chức và người lao động chấm dứt hoặc thay đổi công việc đơn vị phải:

a) Xác định rõ trách nhiệm của cá nhân và các bên liên quan trong quản lý, sử dụng các tài sản công nghệ thông tin được giao.

b) Lập biên bản bàn giao tài sản công nghệ thông tin.

c) Thay đổi hoặc thu hồi quyền truy cập các hệ thống thông tin, phần mềm.

d) 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 QUẢN LÝ THIẾT KẾ, XÂY DỰNG HỆ THỐNG

Điều 9. Thiết kế an toàn hệ thống thông tin

Khi thực hiện triển khai đầu tư, nâng cấp, mở rộng hệ thống hệ thống thông tin, cần thực hiện xây dựng các tài liệu mô tả các yêu cầu sau:

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

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

3. Xây dựng tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ.

4. Xây dựng tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin của hệ thống thông tin thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

5. Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống, báo cáo Lãnh đạo quyết định trước khi thực hiện thay đổi.

Điều 10. Phát triển phần mềm thuê khoán

1. Yêu cầu có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán.

2. Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm.

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

4. Kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng.

Điều 11. Thử nghiệm và nghiệm thu hệ thống

1. Bên triển khai xây dựng kế hoạch, nội dung, quy trình, có bộ phận chịu trách nhiệm thử nghiệm và nghiệm thu hệ thống.

2. Đơn vị vận hành thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác theo phương án thiết kế được phê duyệt trong Hồ sơ đề xuất cấp độ.

3. Cán bộ phụ trách công nghệ thông tin, an toàn thông tin và bên triển khai hệ thống xây dựng kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống, có

báo cáo nghiệm thu được Chủ quản hệ thống thông tin phê duyệt trước khi đưa hệ thống vào vận hành, khai thác.

4. Cán bộ phụ trách công nghệ thông tin, an toàn thông tin phối hợp với 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 nghiệm thu hệ thống.

Điều 12. Bảo đảm an toàn thông tin khi tiếp nhận, phát triển, vận hành và bảo trì hệ thống thông tin

1. Khi thực hiện nâng cấp, mở rộng, thay thế một phần hệ thống thông tin, phải rà soát cấp độ, phương án bảo đảm an toàn của hệ thống thông tin và thực hiện điều chỉnh, bổ sung hoặc thay mới hồ sơ đề xuất cấp độ trong trường hợp cần thiết.

2. Khi tiếp nhận, phát triển, nâng cấp, bảo trì hệ thống thông tin, đơn vị phải tiến hành phân tích, xác định rủi ro có thể xảy ra, đánh giá phạm vi tác động và phải chuẩn bị các biện pháp hạn chế, loại trừ các rủi ro này và yêu cầu các bên cung cấp, thi công, các cá nhân liên quan thực hiện.

3. Trong quá trình vận hành hệ thống thông tin, đơn vị chủ quản hệ thống thông tin cần thực hiện đánh giá, phân loại hệ thống thông tin theo cấp độ; triển khai phương án bảo đảm an toàn hệ thống thông tin đáp ứng yêu cầu cơ bản trong tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm an toàn hệ thống thông tin theo cấp độ; thường xuyên kiểm tra, giám sát an toàn hệ thống thông tin; tuân thủ quy trình vận hành, quy trình xử lý sự cố đã xây dựng; ghi lại và lưu trữ đầy đủ thông tin nhật ký hệ thống để phục vụ quản lý, kiểm soát thông tin.

4. Các cơ quan, đơn vị trực thuộc, tuân thủ các quy định về đảm bảo an toàn thông tin của quy chế này; đảm bảo an toàn thông tin cho toàn bộ hệ thống, tránh lộ, lọt dữ liệu, tài liệu thiết kế, quản trị hệ thống mà đối tác đang xử lý ra bên ngoài.

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

Điều 13. Quản lý an toàn mạng

1. Hoạt động của hệ thống phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của hệ thống.

2. Toàn bộ cấu hình hệ thống phải được sao lưu, dự phòng trên thiết bị hoặc hệ thống lưu trữ độc lập, định kỳ tối thiểu 01 tháng/lần hoặc theo quy định từng nội dung liên quan.

3. Khi thực hiện nâng cấp, thay đổi cấu hình hệ thống phải thực hiện ngoài giờ làm việc.

4. Phải kiểm tra hoạt động tổng thể của hệ thống sau khi thay đổi cấu hình hoặc nâng cấp hệ thống.

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

a) Định kỳ hằng tháng hoặc khi có thay đổi, cán bộ/đơn vị phụ trách công nghệ thông tin, an toàn thông tin thực hiện sao lưu, dự phòng hệ thống trên hệ thống độc lập như: ổ cứng di động hoặc SAN, NAS hoặc các thiết bị lưu trữ khác.

b) Các dữ liệu sau yêu cầu sao lưu, dự phòng: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

6. Truy cập và quản lý cấu hình hệ thống:

a) Cấu hình hệ thống từ xa phải sử dụng các giao thức bảo mật có mã hóa thông tin như SSL, TLS, SSH, VPN.

b) Khi cấu hình hệ thống từ bên ngoài phải thông qua kết nối VPN và được mã hóa trên giao thức đường truyền theo đúng các quy định về bảo mật truy cập từ xa.

c) Toàn bộ cấu hình hệ thống phải được lưu trên thiết bị hoặc hệ thống lưu trữ độc lập.

d) Thiết lập, phân quyền đối với các tài khoản truy cập hệ thống và được sự đồng ý từ quản trị hệ thống.

đ) Ghi và lưu trữ nhật ký hệ thống trong thời gian tối thiểu 90 ngày với những thông tin cơ bản: tên tài khoản, địa chỉ, nhật ký hoạt động và thao tác, các lỗi phát sinh trong quá trình hoạt động,…

Điều 14. Quản lý an toàn máy chủ và ứng dụng

Quy định về quản lý an toàn máy chủ và ứng dụng:

1. Quy định với máy chủ

a) Hoạt động của máy chủ phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của ứng dụng.

b) Ảnh hệ điều hành phải được sao lưu dự phòng trên hệ thống lưu trữ độc lập định kỳ tối thiểu 01 tháng/lần.

c) Máy chủ phải được nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng.

d) Việc kết nối, gỡ bỏ máy chủ khỏi hệ thống phải được sự cho phép của Thủ trưởng đơn vị và xóa sạch dữ liệu.

đ) Có tài liệu liệt kê, cài đặt với những phần mềm hệ thống cài trong máy chủ.

2. Quy định với ứng dụng:

a) Hoạt động của ứng dụng phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của ứng dụng.

b) Ứng dụng phải được thiết lập chính sách xác thực; Kiểm soát truy cập; Có phương án bảo mật thông tin liên lạc và biện pháp bảo đảm an toàn ứng dụng và mã nguồn.

c) Ứng dụng phải được định kỳ kiểm tra đánh giá an toàn thông tin tối thiểu

01 năm/lần hoặc khi thay đổi, nâng cấp mở rộng.

3. Truy cập mạng của máy chủ:

a) Kết nối, truy cập máy chủ phải được kiểm soát bởi tường lửa hệ thống.

b) Chỉ mở cổng quản trị hệ thống từ vùng mạng LAN hoặc vùng mạng quản trị (nếu có).

c) Truy cập quản trị máy chủ từ bên ngoài mạng phải qua kênh kết nối VPN. Các máy tính truy cập từ xa phải đảm bảo an toàn bảo mật thông tin trên đường truyền kết nối và cài đặt các phần mềm anti-virus.

d) Phân quyền, quy định thời gian kết nối đối với các tài khoản kết nối.

4. Truy cập và quản trị máy chủ và ứng dụng:

a) Phải thay đổi ngay mật khẩu mặc định sau khi đưa vào sử dụng và định kỳ thay đổi từ 03 đến 06 tháng.

b) Chỉ cấp quyền quản lý máy chủ và ứng dụng cho công chức, viên chức quản trị theo chức năng nhiệm vụ được giao.

c) Truy cập quản trị máy chủ và ứng dụng phải qua giao thức mã hóa như SSL, TLS, SSH và VPN.

d) Truy cập quản trị máy chủ và ứng dụng từ bên ngoài mạng phải qua kênh kết nối VPN.

đ) Các máy tính quản trị hệ thống phải cài đặt các phần mềm phòng chống mã độc có bản quyền (anti-virus) và phải quét mã độc trước khi kết nối vào hệ thống.

e) Phân quyền, quy định thời gian kết nối đối với các tài khoản quản trị.

5. Quy định về cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố:

a) Định kỳ hằng tháng hoặc khi nâng cấp ứng dụng phải sao lưu, dự phòng mã nguồn ứng dụng và cơ sở dữ liệu trên thiết bị hoặc hệ thống độc lập.

b) Dữ liệu lưu trữ phải được mã hóa cùng mã kiểm tra tính nguyên vẹn.

c) Dữ liệu lưu trữ phải được quản lý theo phiên bản và có quản lý truy cập.

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

a) Kiểm soát và theo dõi tất cả các phương pháp truy cập từ xa tới hệ thống thông tin, triển khai nhiều cơ chế giám sát, cam kết từ các truy cập từ xa; phát hiện sớm việc truy cập trái phép vào mạng máy tính hay thiết bị lưu trữ dữ liệu.

b) Cấu hình hệ thống thông tin cung cấp những chức năng cơ bản cho người dùng; thiết lập các chế độ phân quyền truy cập theo chỉ đạo của Thủ trưởng đơn vị.

Điều 15. Quản lý an toàn dữ liệu

1. Quy định dự phòng và khôi phục dữ liệu:

a) Định kỳ hằng tuần, tháng phải sao lưu, dự phòng cơ sở dữ liệu và dữ liệu nghiệp vụ (nếu có) trên thiết bị hoặc hệ thống độc lập.

b) Phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau.

2. Định kỳ hằng tháng 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.

3. Bản sao lưu được lưu trữ trên thiết bị hoặc hệ thống độc lập.

4. Bố trí máy tính riêng, đặt mật khẩu, mã hóa dữ liệu và các biện pháp bảo mật khác bảo đảm an toàn thông tin khi lưu trữ và truy cập cơ sở dữ liệu hệ thống.

5. Nghiêm cấm các hành vi chia sẻ các tài liệu, dữ liệu liên quan đến hệ thống thông tin của UBND xã khi chưa được sự cho phép của lãnh đạo, người có thẩm quyền và chưa được mã hóa.

Điều 16. Quản lý an toàn thiết bị đầu cuối

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

2. 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.

3. 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 17. 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 phát hiện ra bất kỳ dấu hiện 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 để xử lý.

3. 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.

4. 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 18. Quản lý giám sát an toàn hệ thống thông tin

1. Các hệ thống thông tin đặt tại UBND xã bắt buộc phải có chức năng ghi và lưu trữ nhật ký về hoạt động của hệ thống và người sử dụng hệ thống thông tin. Thực hiện việc bảo vệ các chức năng ghi nhật ký và thông tin nhật ký, chống

giả mạo, sửa đổi, phá hủy và truy cập trái phép.

2. Nguyên tắc, yêu cầu, nội dung, phương thức, hệ thống kỹ thuật phục vụ công tác giám sát thực hiện theo đúng quy định tại Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông quy định hoạt động giám sát An toàn hệ thống thông tin và hướng dẫn triển khai theo Công văn số 2973/BTTTT-CATTT ngày 04/9/2019 của Bộ Thông tin và Truyền thông.

3. Đối tượng giám sát về cơ bản bao gồm máy chủ, thiết bị mạng, thiết bị bảo mật, máy chủ, dịch vụ, ứng dụng, các thiết bị đầu cuối và điểm giám sát đường truyền, cụ thể: giám sát lớp mạng, giám sát lớp máy chủ, giám sát lớp ứng dụng và giám sát lớp đầu cuối.

4. Phải đảm bảo được thực hiện thường xuyên, liên tục. Chủ động theo dõi, phân tích, phòng ngừa nhằm kịp thời phát hiện, ngăn chặn rủi ro, sự cố an toàn thông tin mạng.

5. Đảm bảo ổn định, bí mật cho thông tin cung cấp, trao đổi trong quá trình giám sát.

Điều 19. Quản lý điểm yếu an toàn thông tin

1. 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.

2. Báo cáo Lãnh đạo/Người 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 làm ảnh hưởng/gián đoạn hoạt động của hệ thống.

3. 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.

4. 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.

5. 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.

6. Định kỳ 01 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.

Điều 20. Quản lý sự cố an toàn thông tin

1. Thực hiện cô lập hệ thống, ngắt kết nối với các hệ thống liên quan khác.

2. Khi có sự cố an toàn thông tin xảy ra, cán bộ/đơn vị phụ trách công

nghệ thông tin, an toàn thông tin phải sao lưu, dự phòng toàn bộ hiện trạng hệ thống trước khi xử lý sự cố.

3. Liên hệ với phòng PA05 - Công an tỉnh Lạng Sơn để được hỗ trợ.

Điều 21. Quản lý an toàn người sử dụng đầu cuối

1. Người sử dụng có trách nhiệm tự bảo vệ thông tin cá nhân của mình. Khi sử dụng, khai thác các hệ thống thông tin của cơ quan, đơn vị và các phần mềm ứng dụng dùng chung đặt tại UBND xã, có trách nhiệm:

a) Tự quản lý và chịu trách nhiệm về bảo vệ thông tin cá nhân đã được khai báo trong các hệ thống thông tin; không tiết lộ tài khoản đăng nhập, đấu nối, truy cập trái phép vào các phần mềm dùng chung.

b) Phải thực hiện việc đổi mật khẩu ngay sau khi được cấp tài khoản truy cập vào các phần mềm dùng chung, cơ quan, đơn vị.

c) Khi khai thác, sử dụng các phần mềm dùng chung tại các điểm truy cập Internet công cộng, tuyệt đối không đặt chế độ lưu trữ mật khẩu trong quá trình sử dụng.

2. Các cơ quan, đơn vị, cá nhân khi xử lý thông tin cá nhân phải tuân thủ đầy đủ các quy định:

a) Quản lý và phân quyền truy cập trong các phần mềm ứng dụng, hệ thống thông tin, cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ, quyền hạn của người tham gia quản lý, vận hành, khai thác, sử dụng các phần mềm ứng dụng, hệ thống thông tin, cơ sở dữ liệu.

b) Khi công chức, viên chức đã nghỉ việc hoặc chuyển công tác, các cơ quan, đơn vị phải thực hiện việc thu hồi các thiết bị công nghệ thông tin liên quan; đồng thời phải thông báo ngay bằng văn bản đến cơ quan quản lý, quản trị phần mềm ứng dụng, hệ thống thông tin, cơ sở dữ liệu để thực hiện các biện pháp kỹ thuật cập nhật lại, khóa hoặc hủy tài khoản người dùng.

3. Các đơn vị thuộc UBND xã phải thường xuyên kiểm tra, giám sát các hoạt động chia sẻ, gửi, nhận thông tin, dữ liệu trong hoạt động nội bộ của mình. Khuyến cáo việc chia sẻ, gửi, nhận thông tin trên môi trường mạng cần phải sử dụng mật khẩu để bảo vệ thông tin.

4. Đối với hoạt động trao đổi thông tin, dữ liệu với bên ngoài, đơn vị và cá nhân thực hiện trao đổi thông tin, dữ liệu ra bên ngoài cam kết và có biện pháp bảo mật thông tin, dữ liệu được trao đổi.

Điều 22. Quản lý rủi ro an toàn thông tin mạng

Đơn vị vận hành xây dựng và ban hành Hồ sơ Quản lý rủi ro an toàn thông tin bao gồm các nội dung sau:

1. Danh mục tài sản thông tin, dữ liệu có trong hệ thống.

2. Đánh giá các rủi ro an toàn thông tin đối với mỗi loại tài sản.

3. Có phương án dự phòng và khôi phục sau sự cố đối với thông tin, dữ

liệu và ứng dụng.

Việc kiểm tra, đánh giá và quản lý rủi ro cần tuân thủ các nội dung sau:

a) 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.

Điều 23. Quy định về tài khoản, mật khẩu và phân quyền

1. Phân loại tài khoản

Tài khoản cấp cho cá nhân cán bộ/công chức, viên chức sử dụng, phục vụ theo nhiệm vụ được giao (tài khoản đăng nhập máy tính, tài khoản quản trị máy chủ, tài khoản quản trị thiết bị, tài khoản truy cập ứng dụng nghiệp vụ,…).

2. Nguyên tắc đặt tên tài khoản

Tên tài khoản cấp cho cá nhân cán bộ/công chức, viên chức: Tên tài khoản được đặt đảm bảo được yếu tố định danh duy nhất đến cán bộ/công chức, viên chức quản lý sử dụng tài khoản, trong đó bao gồm nhưng không giới hạn các thông tin: email hoặc mã số cán bộ/công chức, thông tin xác định đơn vị làm việc.

3. Quy định về mật khẩu của tài khoản

Mật khẩu của các tài khoản phải đảm bảo yếu tố mật khẩu mạnh như sau: độ dài mật khẩu: tối thiểu 08 ký tự, mật khẩu phải bao gồm chữ La Mã, số, chữ viết hoa và ký tự đặc biệt. Mật khẩu không được chứa thông tin của tài khoản hoặc các thông tin dễ đoán.

Đối với các mật khẩu mặc định của thiết bị, máy chủ, ứng dụng, cá nhân được giao phụ trách phải thực hiện đổi mật khẩu mặc định ngay lần truy cập đầu tiên, mật khẩu được đổi phải đáp ứng yếu tố mật khẩu mạnh.

4. Đối tượng được cấp tài khoản

Cán bộ/công chức, viên chức đang làm việc thuộc UBND xã được cấp các tài khoản liên quan sử dụng theo nhiệm vụ được phân công.

Đối với các tài khoản quản trị thiết bị, tài khoản quản trị máy chủ, tài khoản quản trị ứng dụng: được cấp cho cá nhân được giao phụ trách thiết bị, máy chủ, ứng dụng theo quyết định phân công nhiệm vụ.

5. Quy định về cấp phát, phân quyền và thu hồi tài khoản

a) Nguyên tắc cấp phát và phân quyền cho tài khoản: Tài khoản được cấp phải gán cho cán bộ/công chức, viên chức chịu trách nhiệm quản lý và sử dụng theo nhiệm vụ được phân công; không cấp tài khoản dùng chung, kể cả tài khoản chỉ có quyền giám sát.

Tài khoản xin cấp và được cấp phát cho cá nhân dựa trên nguyên tắc đảm bảo quyền hạn tối thiểu, vừa đủ cho công việc ứng với vị trí làm việc. Đơn vị cấp phát tài khoản phải xác định thời gian hiệu lực của từng tài khoản được cấp phát.

b) Nguyên tắc thu hồi tài khoản (khóa/xóa tài khoản), thu hồi quyền sử dụng đáp ứng một trong các tiêu chí dưới đây:

- Các tài khoản đã hết thời gian hiệu lực;

- Các tài khoản cấp cho cán bộ/công chức, viên chức đã nghỉ việc hoặc đã chuyển công tác;

- Định kỳ hàng tháng đơn vị vận hành hệ thống thông tin có trách nhiệm rà soát, thu hồi các tài khoản hết hiệu lực, các tài khoản không còn sử dụng.

6. Trách nhiệm quản lý và sử dụng tài khoản

a) Trách nhiệm của đơn vị vận hành hệ thống thông tin:

- Thẩm định các yêu cầu cấp phát tài khoản theo đúng quy định.

- Khai báo các nhóm quyền cho từng thiết bị, hệ thống đảm bảo chặt chẽ, đúng mục đích sử dụng của từng đối tượng.

- Duy trì việc kiểm tra rà soát, thu hồi tài khoản theo đúng quy định.

- Đối với các tài khoản được cấp ngắn hạn phục vụ việc hỗ trợ xử lý sự cố, cập nhật hệ thống,… phải thực hiện thu hồi ngay sau khi hoàn thành công việc.

b) Trách nhiệm của cá nhân sử dụng tài khoản:

- Thiết lập chính sách mật khẩu mạnh cho các tài khoản được cấp theo đúng quy định.

- Chịu trách nhiệm trước người đứng đầu đơn vị trong việc quản lý, sử dụng tài khoản được cấp.

- Có trách nhiệm bảo vệ thông tin của tài khoản được cấp, bảo vệ bí mật của tài khoản.

Điều 24. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

Quy định, quy trình về kết thúc vận hành, khai thác, thanh lý, hủy bỏ bao gồm các nội dung sau:

1. Thiết bị công nghệ thông tin có chứa dữ liệu (máy tính, thiết bị lưu trữ, ...) khi bị hỏng phải được công chức 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.

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

3. Các phương tiện và thiết bị công nghệ thông tin: 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
TỔ CHỨC BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 25. Trách nhiệm của các cơ quan, đơn vị thuộc UBND xã

1. Phổ biến và triển khai các hệ thống thông tin tại đơn vị tuân thủ các quy định tại Quy chế này và các văn bản quy định có liên quan khác của pháp luật về an toàn thông tin mạng.

2. Đối với các đơn vị có hệ thống thông tin: mạng LAN, hệ thống cơ sở dữ liệu, máy chủ,…; triển khai áp dụng quy chế này tại đơn vị và ban hành văn bản hướng dẫn tổ chức thực hiện, trong đó bao gồm việc giao nhiệm vụ cụ thể cho bộ phận, cá nhân thực hiện công tác bảo đảm an toàn, an ninh thông tin mạng. Tùy theo mô hình quản lý, tính chất của hệ thống thông tin, các đơn vị xây dựng, ban hành quy chế đảm bảo an toàn thông tin mạng tại đơn vị (nếu cần).

3. Xây dựng sơ đồ tổng thể, đánh giá hiện trạng và bổ sung các thành phần trong hệ thống: thiết bị mạng, bảo mật, máy chủ, thiết bị đầu cuối, thông tin tài liệu… đảm bảo an toàn cho các hệ thống thông tin, tài liệu… và xây dựng hồ sơ đề xuất cấp độ cho hệ thống thông tin tại đơn vị.

4. Thường xuyên kiểm tra việc thực hiện Quy chế này tại đơn vị, coi đây là nhiệm vụ trọng tâm của đơn vị; chịu trách nhiệm trước pháp luật và Lãnh đạo UBND xã về các vi phạm, thất thoát thông tin, dữ liệu mật thuộc phạm vi quản lý của đơn vị do không tổ chức, chỉ đạo, kiểm tra cán bộ, công chức, viên chức của đơn vị thực hiện đúng quy định.

5. Chủ trì, phối hợp với Văn phòng HĐND và UBND xã trong việc bảo đảm an toàn thông tin trong quá trình triển khai hệ thống thông tin.

6. Cán bộ, công chức, viên chức, người lao động có trách nhiệm: tuân thủ Quy chế này; thông báo kịp thời các vấn đề bất thường liên quan đến an toàn thông tin cho cán bộ/đơn vị phụ trách công nghệ thông tin, an toàn thông tin về an toàn thông tin mạng tại cơ quan.

7. Tùy theo tình hình thực tế, các đơn vị có thể áp dụng Quy chế cho các hệ thống thông tin đã triển khai theo các dự án đầu tư công nghệ thông tin hoặc hệ thống thông tin đã có quy định riêng.

Điều 26. Trách nhiệm của Văn phòng HĐND và UBND xã

1. Định kỳ hướng dẫn triển khai Quy chế này và các quy định pháp luật có liên quan.

2. Tổ chức triển khai Quy chế cho các hệ thống thông tin tại UBND xã.

3. Xây dựng hồ sơ đề xuất cấp độ cho hệ thống thông tin tại cơ quan theo quy định và gửi Công an tỉnh đề xuất phê duyệt cấp độ.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 27. Xây dựng và công bố

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

2. Trong quá trình thực hiện nếu có vấn đề phát sinh, vướng mắc, các cơ quan, đơn vị liên quan, cán bộ, công chức, viên chức, người lao động phản ánh kịp thời về Văn phòng HĐND và UBND xã để xem xét, đề xuất sửa đổi, bổ sung.

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

1. Định kỳ 02 năm hoặc khi có quy định, chính sách mới cần điều chỉnh, bổ sung Quy chế bảo đảm an toàn thông tin, Văn phòng HĐND và UBND xã tham mưu rà soát, cập nhật, bổ sung quy chế phù hợp.

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. Phổ biến đến toàn thể cán bộ, công chức, viên chức, người lao động thuộc đối tượng áp dụng tại Điều 2./.

CÁC BIỂU MẪU

1. Biểu mẫu biên bản bàn giao tài sản, trang thiết bị CNTT

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

BIÊN BẢN BÀN GIAO TÀI SẢN, TRANG THIẾT BỊ CNTT
(Số:…….)

Căn cứ.....

Căn cứ Quy chế Bảo đảm an toàn thông tin mạng nội bộ tại .....,

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

BÊN GIAO: ……

Họ và tên : .....
Chức vụ : .....
Đơn vị : ……..
Số điện thoại : ……..

BÊN NHẬN: .....

Họ và tên : .....
Chức vụ : .....
Đơn vị : ……..
Số điện thoại : ……..
Họ và tên : .....

Hai Bên cùng thống nhất ký kết biên bản bàn giao tài sản, trang thiết bị CNTT chi tiết như sau:

1. Nội dung bàn giao: Tài sản, trang thiết bị công nghệ thông tin chi tiết chủng loại, số lượng như sau:

#	Tên tài sản/thiết bị	Model/cấu hình	Hãng/xuất xứ	Serial	Số lượng	Tình trạng	Ghi chú
1	…	…	…	…	…	…	…
2	…	…	…	…	…	…	…

2. Cam kết :

- Hai Bên đã tiến hành kiểm tra về chủng loại, số lượng tài sản, trang thiết bị CNTT theo đúng nội dung bàn giao.
- Bên nhận có trách nhiệm quản lý, sử dụng tài sản, trang thiết bị CNTT đúng mục đích, không tự ý thay đổi cấu hình, cài đặt các phần mềm trái quy định.
- Bên nhận có trách nhiệm bảo quản sử dụng tài sản theo đúng quy định.
- Bên giao có trách nhiệm đào tạo hướng dẫn sử dụng, bàn giao tài khoản và các thông tin, giấy tờ khác có liên quan đến tài sản, trang thiết bị CNTT cho bên nhận.

Biên bản này được lập thành …. bản có giá trị pháp lý như nhau, mỗi Bên giữ … bản./.

ĐẠI DIỆN BÊN GIAO **ĐẠI DIỆN BÊN NHẬN**

2. Biểu mẫu cam kết người dùng

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

CAM KẾT
v/v tuân thủ quy định bảo mật, an toàn thông tin mạng nội bộ

Căn cứ.....

Căn cứ Quy chế Bảo đảm an toàn thông tin mạng nội bộ tại .....,

Họ và tên : .....

Chức vụ : .....

Đơn vị : ……..

Số điện thoại : ……..

Cam kết :

- Tuân thủ các quy định về bảo mật, an toàn thông tin theo quy định của pháp luật và Quy chế bảo đảm an toàn thông tin, an ninh mạng nội bộ tại đơn vị.
- Sử dụng tài khoản, trang thiết bị CNTT đúng mục đích công việc.
- Không tự ý lắp đặt cài đặt các phần mềm, thiết bị CNTT khi chưa được phép.
- Chịu trách nhiệm trước pháp luật và đơn vị về việc bảo mật thông tin cá nhân, thông tin khách hàng thuộc phạm vi quản lý.
- ……

Tôi cam kết chấp hành và chịu hoàn toàn trách nhiệm với các nội dung đã nêu trên.

……ngày…….tháng….năm……

NGƯỜI CAM KẾT

3. Biểu mẫu nhật ký vận hành hệ thống

NHẬT KÝ VẬN HÀNH HỆ THỐNG CNTT

Đơn vị vận hành: ……..
Cá nhân được giao vận hành: ……..
Tên hệ thống: …….

#	Thời gian	Nội dung kiểm tra/vận hành	Kết quả	Người thực hiện	Ghi chú
1	23/4/2026	Cập nhật firmware cho thiết bị firewall S-Gate, phiên bản 39.5.2	Thành công	Nguyễn Văn A	Theo dõi hệ thống hoạt động ổn định
2	…	…	…	…	…

4. Nhật ký xử lý sự cố

NHẬT KÝ XỬ LÝ SỰ CỐ

Đơn vị vận hành: ……..
Cá nhân được giao vận hành: ……..

#	Thời gian	Nguồn sự cố	Nội dung sự cố	Mức độ	Phương án xử lý	Kết quả	Người xử lý	Ghi chú
1	…	…	…	…	…	…	…	…
2	…	…	…	…				…