ỦY BAN NHÂN DÂN XÃ ĐƯỜNG AN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 949/QĐ-UBND	*Đường An, ngày 05 tháng 6 năm 2026*

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn thông tin mạng và an toàn hệ thống thông tin của UBND xã Đường An

CHỦ TỊCH ỦY BAN NHÂN DÂN XÃ ĐƯỜNG AN

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 các quy định của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ các quy định của thành phố Hải Phòng về bảo đảm an toàn thông tin, an ninh mạng và bảo vệ bí mật nhà nước;

Căn cứ Quyết định số 6841/QĐ-CAHP-ANM ngày 29/5/2026 về việc phê duyệt cấp độ an toàn hệ thống thông tin của UBND xã Đường An;

Theo đề nghị của Chánh Văn phòng HĐND và UBND xã Đường An.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Quy chế bảo đảm an toàn thông tin mạng và an toàn hệ thống thông tin của UBND xã Đường An".

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

Điều 3. Chánh Văn phòng HĐND và UBND xã; Trưởng các phòng chuyên môn; người đứng đầu các cơ quan, đơn vị thuộc UBND xã; cán bộ, công chức, viên chức, người lao động và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Thường trực ĐU xã;
- Thường trực HĐND xã;
- Chủ tịch và các PCT xã;
- Lưu: VT, VP.

CHỦ TỊCH

U.B.N.D XÃ ĐƯỜNG AN T.P HẢI PHÒNG

Đào Đức Vỹ

QUY CHẾ
Bảo đảm an toàn thông tin mạng và an toàn hệ thống thông tin của Ủy ban nhân dân xã Đường An

(*Ban hành kèm theo Quyết định số 949/QĐ-UBND ngày 05 tháng 6 năm 2026*)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

1. Quy chế này quy định việc bảo đảm an toàn thông tin mạng và an toàn hệ thống thông tin tại UBND xã Đường An; quản lý, vận hành, khai thác và sử dụng các hệ thống thông tin, mạng nội bộ, thiết bị công nghệ thông tin, tài khoản, dữ liệu và các dịch vụ số thuộc phạm vi quản lý của UBND xã.

2. Quy chế là cơ sở để phòng ngừa, phát hiện, xử lý và khắc phục các nguy cơ, sự cố mất an toàn thông tin trong hoạt động của UBND xã.

Điều 2. Đối tượng áp dụng

Quy chế này áp dụng đối với cán bộ, công chức, viên chức, người lao động thuộc UBND xã và các tổ chức, cá nhân có liên quan đến việc quản lý, vận hành, khai thác, sử dụng hệ thống thông tin, mạng và thiết bị công nghệ thông tin của UBND xã Đường An.

Điều 3. Nguyên tắc bảo đảm an toàn thông tin

1. Bảo đảm an toàn thông tin là trách nhiệm của người đứng đầu cơ quan, đơn vị và của từng cán bộ, công chức, người sử dụng hệ thống.

2. Việc quản lý, khai thác và sử dụng hệ thống thông tin phải bảo đảm tính bí mật, toàn vẹn và khả dụng của thông tin, dữ liệu.

3. Thực hiện bảo đảm an toàn thông tin theo cấp độ đã được cơ quan có thẩm quyền phê duyệt; chủ động phòng ngừa, phát hiện và xử lý kịp thời các nguy cơ, sự cố.

4. Không sử dụng hệ thống thông tin, thiết bị và tài khoản của cơ quan vào các hoạt động trái quy định của pháp luật hoặc làm ảnh hưởng đến an toàn, an ninh mạng.

Chương II
QUẢN LÝ VÀ SỬ DỤNG HỆ THỐNG THÔNG TIN

Điều 4. Quản lý hệ thống thông tin

1. UBND xã tổ chức quản lý, vận hành và bảo đảm an toàn đối với Hệ thống thông tin UBND xã Đường An theo cấp độ đã được phê duyệt.

2. Văn phòng HĐND và UBND xã là đầu mối tham mưu, phối hợp quản lý, vận hành và bảo đảm an toàn hệ thống thông tin của UBND xã.

3. Cán bộ được giao phụ trách công nghệ thông tin, an toàn thông tin thực hiện nhiệm vụ theo phân công; theo dõi tình trạng hoạt động của hệ thống, thiết bị mạng, máy tính và phối hợp xử lý khi phát sinh sự cố.

4. Các phòng chuyên môn, bộ phận và cá nhân sử dụng hệ thống có trách nhiệm chấp hành các quy định về bảo đảm an toàn thông tin.

Điều 5. Quản lý tài khoản và mật khẩu

1. Mỗi cán bộ, công chức sử dụng tài khoản được cấp để thực hiện nhiệm vụ; không sử dụng chung tài khoản khi hệ thống yêu cầu tài khoản cá nhân.

2. Không cung cấp, chia sẻ tài khoản, mật khẩu cho người khác dưới bất kỳ hình thức nào.

3. Mật khẩu phải có độ phức tạp phù hợp, không sử dụng các thông tin dễ đoán như họ tên, ngày sinh, số điện thoại hoặc các thông tin cá nhân phổ biến.

4. Khi phát hiện tài khoản có dấu hiệu bị lộ, bị chiếm quyền sử dụng hoặc sử dụng bất thường, phải thông báo ngay cho cán bộ phụ trách CNTT để xử lý.

5. Khi cán bộ chuyển công tác, nghỉ việc hoặc thay đổi nhiệm vụ, tài khoản phải được rà soát, điều chỉnh hoặc thu hồi theo quy định.

Điều 6. Quản lý máy tính và thiết bị công nghệ thông tin

1. Máy tính được sử dụng để xử lý công việc phải được cài đặt phần mềm bảo vệ, cập nhật hệ điều hành và phần mềm cần thiết theo quy định.

2. Không tự ý cài đặt phần mềm không rõ nguồn gốc hoặc phần mềm có nguy cơ gây mất an toàn thông tin.

3. Không tự ý tháo lắp, thay đổi cấu hình thiết bị mạng, máy chủ, thiết bị bảo mật và các thiết bị công nghệ thông tin thuộc cơ quan.

4. Thiết bị lưu trữ dữ liệu phải được kiểm tra trước khi kết nối với máy tính của cơ quan.

5. Khi rời khỏi vị trí làm việc, cán bộ, công chức phải khóa máy tính hoặc thực hiện biện pháp bảo vệ phù hợp.

Điều 7. Quản lý mạng và kết nối Internet

1. Mạng nội bộ và kết nối Internet của UBND xã được quản lý tập trung, bảo đảm an toàn và phục vụ hoạt động công vụ.

2. Không tự ý kết nối thiết bị cá nhân hoặc thiết bị không được kiểm soát vào hệ thống mạng nội bộ khi chưa được phép.

3. Không truy cập, tải xuống hoặc phát tán nội dung có nguy cơ gây mất an toàn thông tin, mã độc hoặc các nội dung vi phạm pháp luật.

4. Cán bộ phụ trách CNTT thường xuyên kiểm tra tình trạng hoạt động của hệ thống mạng, thiết bị mạng và phối hợp với đơn vị cung cấp dịch vụ khi có sự cố.

Chương III
BẢO VỆ DỮ LIỆU VÀ THÔNG TIN

Điều 8. Quản lý, bảo vệ dữ liệu

1. Dữ liệu của UBND xã phải được quản lý, lưu trữ và khai thác đúng chức năng, nhiệm vụ và thẩm quyền.

2. Không tự ý sao chép, cung cấp, chuyển giao hoặc đưa dữ liệu của cơ quan lên các hệ thống, nền tảng hoặc dịch vụ không được phép.

3. Dữ liệu quan trọng phải được sao lưu theo kế hoạch hoặc yêu cầu của hệ thống; bảo đảm khả năng khôi phục khi xảy ra sự cố.

4. Khi trao đổi dữ liệu điện tử phải sử dụng các hệ thống, nền tảng được cơ quan có thẩm quyền cho phép.

Điều 9. Bảo vệ thông tin cá nhân và dữ liệu dân cư

1. Việc thu thập, quản lý, khai thác và sử dụng thông tin cá nhân, dữ liệu dân cư phải đúng mục đích, đúng thẩm quyền và theo quy định của pháp luật.

2. Không tự ý chụp ảnh, sao chép, tải xuống, lưu trữ hoặc chia sẻ dữ liệu cá nhân của tổ chức, công dân khi không phục vụ nhiệm vụ được giao.

3. Khi phát hiện nguy cơ lộ, mất hoặc sử dụng trái phép dữ liệu cá nhân phải báo cáo ngay người có thẩm quyền và cán bộ phụ trách ATTT để xử lý.

Điều 10. Bảo vệ bí mật nhà nước

1. Việc quản lý, lưu trữ, trao đổi, truyền đưa và xử lý thông tin thuộc phạm vi bí mật nhà nước phải thực hiện theo quy định của pháp luật về bảo vệ bí mật nhà nước.

2. Không sử dụng máy tính, mạng, thư điện tử hoặc thiết bị không bảo đảm điều kiện an toàn để xử lý thông tin bí mật nhà nước.

3. Máy tính, thiết bị và hệ thống dùng để xử lý thông tin bí mật nhà nước phải được quản lý riêng và thực hiện các biện pháp bảo vệ theo quy định.

Chương IV
BẢO ĐẢM AN TOÀN TRONG VẬN HÀNH

Điều 11. Bảo vệ nhiều lớp

UBND xã thực hiện các biện pháp bảo vệ nhiều lớp phù hợp với hệ thống, gồm:

1. Bảo vệ thiết bị mạng và kết nối Internet.

2. Quản lý tài khoản, phân quyền truy cập.

3. Cài đặt và duy trì phần mềm phòng, chống mã độc.

4. Cập nhật hệ điều hành, phần mềm và bản vá bảo mật.

5. Sao lưu, phục hồi dữ liệu.

6. Kiểm tra, giám sát và phát hiện các dấu hiệu bất thường.

7. Các biện pháp bảo vệ khác theo phương án bảo đảm an toàn hệ thống thông tin cấp độ 2 được phê duyệt.

Điều 12. Sao lưu và phục hồi dữ liệu

1. Dữ liệu quan trọng phải được sao lưu định kỳ theo yêu cầu của từng hệ thống.

2. Bản sao lưu phải được quản lý, bảo vệ, hạn chế truy cập trái phép.

3. Khi xảy ra sự cố làm mất hoặc hỏng dữ liệu, cán bộ phụ trách phối hợp với đơn vị liên quan thực hiện khôi phục dữ liệu từ bản sao lưu.

Điều 13. Quản lý phần mềm và cập nhật bảo mật

1. Chỉ sử dụng phần mềm có nguồn gốc hợp pháp, được phép sử dụng.

2. Thường xuyên cập nhật hệ điều hành, phần mềm và các bản vá bảo mật theo hướng dẫn của nhà cung cấp hoặc cơ quan chuyên môn.

3. Không sử dụng phần mềm bẻ khóa, phần mềm không rõ nguồn gốc trên thiết bị phục vụ công việc.

Chương V
PHÒNG NGỪA VÀ XỬ LÝ SỰ CỐ AN TOÀN THÔNG TIN

Điều 14. Phát hiện và báo cáo sự cố

Các trường hợp sau phải được báo cáo ngay cho cán bộ phụ trách CNTT/ATTT:

1. Máy tính có dấu hiệu nhiễm mã độc, mất dữ liệu hoặc hoạt động bất thường.

2. Tài khoản bị lộ mật khẩu, bị chiếm quyền hoặc đăng nhập bất thường.

3. Phát hiện dữ liệu bị xóa, thay đổi hoặc truy cập trái phép.

4. Hệ thống mạng, phần mềm, cơ sở dữ liệu hoặc các dịch vụ số bị gián đoạn bất thường.

5. Phát hiện nguy cơ lộ thông tin cá nhân, dữ liệu công dân hoặc bí mật nhà nước.

6. Các sự cố khác có nguy cơ ảnh hưởng đến an toàn hệ thống thông tin.

Điều 15. Xử lý sự cố

1. Khi xảy ra sự cố, người phát hiện phải kịp thời thông báo cho người phụ trách và không tự ý thực hiện các biện pháp có thể làm mất dấu vết hoặc làm sự cố nghiêm trọng hơn.

2. Cán bộ phụ trách CNTT/ATTT có trách nhiệm đánh giá sơ bộ, thực hiện biện pháp cô lập, khắc phục ban đầu và báo cáo lãnh đạo UBND xã.

3. Trường hợp sự cố vượt quá khả năng xử lý, Văn phòng HĐND và UBND xã phối hợp với cơ quan chuyên môn của thành phố và đơn vị cung cấp dịch vụ để xử lý.

5. Sau sự cố phải thực hiện đánh giá nguyên nhân, mức độ ảnh hưởng và đề xuất biện pháp phòng ngừa tái diễn.

Chương VI
KIỂM TRA, GIÁM SÁT VÀ ĐÁNH GIÁ AN TOÀN THÔNG TIN

Điều 16. Kiểm tra an toàn thông tin

1. UBND xã tổ chức kiểm tra việc thực hiện Quy chế này và các yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Cán bộ phụ trách CNTT/ATTT định kỳ kiểm tra tình trạng máy tính, mạng, thiết bị bảo mật, phần mềm phòng chống mã độc, tài khoản và các thiết bị công nghệ thông tin.

3. Khi phát hiện nguy cơ mất an toàn thông tin phải kịp thời báo cáo và đề xuất biện pháp xử lý.

Điều 17. Đánh giá và rà soát

1. Hồ sơ xác định cấp độ và phương án bảo đảm an toàn hệ thống thông tin phải được rà soát khi có thay đổi lớn về hệ thống, chức năng, phạm vi hoặc mức độ xử lý thông tin.

2. UBND xã phối hợp thực hiện kiểm tra, đánh giá an toàn thông tin theo yêu cầu của cơ quan có thẩm quyền.

3. Kết quả kiểm tra, đánh giá là cơ sở để khắc phục điểm yếu và nâng cao mức độ an toàn của hệ thống.

Chương VII
TRÁCH NHIỆM CỦA CÁC CƠ QUAN, ĐƠN VỊ, CÁ NHÂN

Điều 18. Trách nhiệm của Chủ tịch UBND xã

1. Chỉ đạo chung công tác bảo đảm an toàn thông tin tại UBND xã.

2. Chỉ đạo tổ chức thực hiện các yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ.

3. Chỉ đạo xử lý các sự cố an toàn thông tin nghiêm trọng.

Điều 19. Trách nhiệm của Chánh Văn phòng HĐND và UBND xã

1. Tham mưu Chủ tịch UBND xã tổ chức thực hiện Quy chế.

2. Chỉ đạo cán bộ phụ trách CNTT/ATTT thực hiện công tác quản lý, vận hành và bảo đảm an toàn hệ thống thông tin.

3. Theo dõi, tổng hợp tình hình ATTT; báo cáo lãnh đạo UBND xã và cơ quan có thẩm quyền khi cần thiết.

Điều 20. Trách nhiệm của cán bộ phụ trách CNTT, ATTT

1. Tham mưu triển khai các biện pháp bảo đảm an toàn hệ thống thông tin theo cấp độ 2.

2. Theo dõi tình trạng hoạt động của mạng, thiết bị và các hệ thống thông tin thuộc phạm vi quản lý.

3. Quản lý, phối hợp quản lý tài khoản, phân quyền và thiết bị CNTT theo nhiệm vụ được giao.

4. Phối hợp xử lý sự cố, khôi phục hoạt động của hệ thống.

5. Tham mưu tổ chức tuyên truyền, hướng dẫn cán bộ, công chức thực hiện các quy định về ATTT.

6. Phối hợp với cơ quan chuyên môn và đơn vị cung cấp dịch vụ trong việc kiểm tra, khắc phục sự cố và nâng cao an toàn hệ thống.

Điều 21. Trách nhiệm của cán bộ, công chức, người lao động

1. Chấp hành Quy chế và các quy định về an toàn thông tin.

2. Bảo vệ tài khoản, mật khẩu và dữ liệu được giao quản lý.

3. Không tự ý cung cấp thông tin, dữ liệu của cơ quan cho tổ chức, cá nhân không có thẩm quyền.

4. Chủ động phát hiện, báo cáo nguy cơ và sự cố ATTT.

5. Chịu trách nhiệm về việc sử dụng tài khoản, thiết bị và dữ liệu trong phạm vi nhiệm vụ được giao.

Chương VIII
TỔ CHỨC THỰC HIỆN

Điều 22. Tổ chức thực hiện

1. Chánh Văn phòng HĐND và UBND xã có trách nhiệm tổ chức triển khai Quy chế đến toàn thể cán bộ, công chức, người lao động thuộc UBND xã.

2. Trưởng các phòng chuyên môn, người đứng đầu các bộ phận, đơn vị thuộc UBND xã chịu trách nhiệm phổ biến và tổ chức thực hiện các quy định về ATTT trong phạm vi phụ trách.

3. Cán bộ, công chức, người lao động có trách nhiệm thực hiện nghiêm Quy chế này.

Điều 23. Khen thưởng và xử lý vi phạm

1. Tập thể, cá nhân thực hiện tốt công tác bảo đảm ATTT được xem xét biểu dương, khen thưởng theo quy định.

2. Tổ chức, cá nhân vi phạm Quy chế, làm mất an toàn thông tin, gây thiệt hại đến hệ thống, dữ liệu hoặc thông tin của cơ quan thì tùy theo tính chất, mức độ vi phạm sẽ bị xử lý theo quy định của pháp luật và quy định của cơ quan.

Điều 24. Sửa đổi, bổ sung Quy chế

Trong quá trình thực hiện, nếu có khó khăn, vướng mắc hoặc có thay đổi về quy định pháp luật, công nghệ, hệ thống thông tin và yêu cầu bảo đảm ATTT, Văn phòng HĐND và UBND xã chủ trì rà soát, tham mưu Chủ tịch UBND xã xem xét sửa đổi, bổ sung Quy chế cho phù hợp./.