ỦY BAN NHÂN DÂN **HUYỆN VĨNH LINH**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 3696/QĐ-UBND	*Vĩnh Linh, ngày 12 tháng 11 năm 2024*

QUYẾT ĐỊNH

Ban hành quy chế đảm bảo an toàn thông tin, an ninh thông tin trong hoạt động ứng dụng CNTT của các cơ quan nhà nước huyện Vĩnh Linh.

ỦY BAN NHÂN DÂN HUYỆN VĨNH LINH

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19/6/2015;

Căn cứ Luật An toàn thông tin mạng ngày 19/11/2015; Luật giao dịch điện tử ngày 22/06/2023; Luật công nghệ thông tin 29/6/2006;

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

Căn cứ quyết định số 35/2016/QĐ-UBND ngày 29/8/2016 của Ủy ban nhân tỉnh về việc ban hành quy chế đảm bảo an toàn thông tin, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Quảng Trị;

Xét đề nghị của Trưởng phòng Văn hóa và Thông tin.

QUYẾT ĐỊNH

Điều 1. Ban hành kèm theo Quyết định này là Quy chế đảm bảo an toàn thông tin, an ninh thông tin trong hoạt động ứng dụng CNTT của các cơ quan nhà nước huyện Vĩnh Linh.

Điều 2. Quyết định này có hiệu lực thi hành sau 10 ngày, kể từ ngày ký.

Chánh Văn phòng HĐND&UBND huyện, Trưởng phòng Văn hóa và Thông tin, Trưởng các phòng, ban, ngành, đoàn thể cấp huyện, Chủ tịch UBND các xã, thị trấn chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- UBND tỉnh;
- Sở Thông tin và Truyền thông;
- TT Huyện ủy, HĐND,UBMTTQVN huyện;
- Điều 3;
- Lưu: VP-VT.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Thái Văn Thành

ỦY BAN NHÂN DÂN **HUYỆN VĨNH LINH**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**

Vĩnh Linh, ngày 12 tháng 11 năm 2024

QUY CHẾ
Đảm bảo an toàn thông tin, an ninh thông tin trong hoạt động ứng dụng CNTT của các cơ quan nhà nước huyện Vĩnh Linh

(Ban hành kèm theo Quyết định số 3696/2024/QĐ-UBND ngày ...12 tháng .11.. năm 2024 của Ủy ban nhân dân huyện Vĩnh Linh)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định các nội dung của công tác đảm bảo an toàn thông tin, an ninh thông tin trong hoạt động ứng dụng CNTT của các cơ quan nhà nước huyện Vĩnh Linh, bao gồm: công tác xây dựng các quy định quản lý đảm bảo an toàn thông tin, an ninh thông tin; việc áp dụng các biện pháp quản lý kỹ thuật, quản lý vận hành đảm bảo an toàn thông tin, an ninh thông tin đối với các hệ thống thông tin.

Điều 2. Đối tượng áp dụng

1. Quy chế này được áp dụng đối với các cơ quan nhà nước huyện Vĩnh Linh bao gồm: các cơ quan chuyên môn, đơn vị sự nghiệp trực thuộc Ủy ban nhân dân huyện, Ủy ban nhân dân các xã, thị trấn.

2. Các tổ chức chính trị, chính trị - xã hội của huyện Vinh Linh.

3. Cán bộ, công chức, viên chức và người lao động đang làm việc trong các cơ quan, đơn vị nêu tại Khoản 1 và 2 Điều này.

4. Cơ quan, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin và an toàn thông tin cho các cơ quan, đơn vị thuộc khoản 1, 2 Điều này.

Điều 3. Giải thích từ ngữ

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

1. *Cơ quan nhà nước huyện Vĩnh Linh:* là các cơ quan chuyên môn, đơn vị sự nghiệp trực thuộc Ủy ban nhân dân huyện, Ủy ban nhân dân các xã, thị trấn; các tổ chức chính trị, chính trị - xã hội thuộc Huyện.

2. *An toàn thông tin*: là sự bảo vệ thông tin, hệ thống thông tin 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.

3.An ninh thông tin: là việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

4. *Hệ thống thông tin:* là một hệ thống bao gồm con người, dữ liệu, các quy trình và công nghệ thông tin tương tác với nhau để thu thập, xử lý, lưu trữ và cung cấp thông tin cần thiết ở đầu ra nhằm hỗ trợ cho một hệ thống.

5. *Tài sản công nghệ thông tin*: là các trang thiết bị, phần mềm, các thiết bị vật lý khác thuộc hệ thống thông tin của đơn vị.

Chương II
QUY ĐỊNH ĐẢM BẢO AN TOÀN THÔNG TIN, AN NINH THÔNG TIN

Điều 1: Cán bộ, công chức, viên chức và người lao động

1. Các phòng, ban, đơn vị và cá nhân phải cam kết, tuân thủ thực hiện các quy chế, quy định quản lý, vận hành, khai thác hạ tầng, phần mềm, cơ sở dữ liệu CNTT và đảm bảo an toàn thông tin, an ninh thông tin trong hoạt động ứng dụng của các cơ quan nhà nước huyện Vĩnh Linh.

2. Khi công chức, viên chức, người lao động chấm dứt hoặc thay đổi công việc, thủ trưởng cơ quan trực tiếp quản lý người lao động phải báo cáo cho Chánh văn phòng UBND&HĐND để xác định rõ trách nhiệm của cá nhân liên quan hệ thống CNTT; thực hiện thu hồi hoặc thay đổi quyền truy cập hệ thống CNTT cho phù hợp. Cơ quan quản lý trực tiếp có văn bản đề nghị thu hồi chứng thư chữ ký số chuyên dùng công vụ.

3. Văn phòng HĐND&UBND huyện có trách nhiệm phối hợp với các cơ quan liên quan tạo, lập và cung cấp tài khoản truy nhập vào các hệ thống thông tin triển khai tại UBND huyện cho các cán bộ, công chức của các cơ quan, đơn vị trên địa bàn huyện.

Điều 2. Quản lý tài sản công nghệ thông tin

1. Hàng năm các cơ quan, đơn vị có kế hoạch kiểm kê, bảo dưỡng, nâng cấp hoặc thay mới tài sản CNTT. Đối với tài sản là trang thiết bị lưu trữ thông tin khi không còn sử dụng cần phải được hủy bỏ, đảm bảo tránh mất mát dữ liệu và không thể phục hồi.

2. Đối với các tài sản CNTT có tính chất quan trọng, trọng yếu, phục vụ công việc có yêu cầu đảm bảo bí mật trước khi đưa vào lắp đặt, cài đặt, vận hành cần phối hợp với các cơ quan chức năng (Phòng Văn hóa và Thông tin; Văn phòng UBND&HĐND huyện; Sở Thông tin và Truyền thông; Công an huyện) thực hiện kiểm tra, đánh giá mức độ an toàn tại hệ thống Công nghệ thông tin.

3. Các đơn vị khi mua sắm, đầu tư tài sản CNTT với bên thứ ba, ngoài việc yêu cầu bên thứ ba cung cấp các dịch vụ, hàng hóa CNTT (tư vấn, mua sắm, bảo dưỡng, sửa chữa tài sản CNTT...) đảm bảo các yêu cầu cung cấp hàng hóa, dịch vụ theo quy định của Nhà nước, còn phải thực hiện việc quản lý đảm bảo an toàn thông tin, an ninh thông tin.

Điều 3. Quản lý phòng máy chủ

1. Các thiết bị mạng quan trọng như tường lửa (firewall), thiết bị định tuyến (router), hệ thống máy chủ, … phải được đặt trong phòng máy chủ và có các biện pháp bảo vệ, ngăn chặn xâm nhập trái phép vào phòng máy chủ. Là khu vực hạn chế tiếp cận và được lắp đặt hệ thống camera giám sát. Chỉ những người có trách nhiệm theo quy

định của thủ trưởng cơ quan mới được phép vào phòng máy chủ.

2. Quá trình vào, ra phòng máy chủ phải được ghi nhận vào nhật ký quản lý phòng máy chủ.

3. Phòng máy chủ phải có hệ thống lưu điện đủ công suất và duy trì thời gian hoạt động của các máy chủ tối thiểu 15 phút khi có sự cố mất điện.

Điều 4. Phòng chống mã độc

1. Tất cả các máy tính phải được trang bị phần mềm phòng chống mã độc và cấu hình nhằm vô hiệu hóa tính năng tự động thực thi (autoplay) các tập tin trên các thiết bị lưu trử di động. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin.

2. Các cán bộ, công chức, viên chức và người lao động trong cơ quan phải được hướng dẫn về phòng chống mã độc, các rủi ro do mã độc gây ra, được tham gia các lớp tập huấn nâng cao năng lực về an toàn thông tin, an ninh thông tin.

3. Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm mã độc trên máy tính (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu,…), người sử dụng phải tắt máy và báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý (*Mỗi cơ quan cử 01 đồng chí làm đầu mối về ATTT, ANTT*).

Điều 5. Sao lưu dữ liệu dự phòng

Các cơ quan phải lập kế hoạch và thực hiện sao lưu dữ liệu định kỳ phù hợp với điều kiện của từng cơ quan, đảm bảo khả năng phục hồi dữ liệu khi có sự cố xảy ra.

Điều 6. Thiết bị tường lửa

1. Các hạ tầng công nghệ thông tin phải được trang bị tường lửa để ngăn chặn và phát hiện các xâm nhập trái phép vào mạng nội bộ.

2. Nhật ký hoạt động của thiết bị tường lửa phải được lưu giữ an toàn để phục vụ công tác khảo sát, điều tra khi có sự cố xảy ra.

Điều 7. Quản lý, vận hành hệ thống thông tin của đơn vị

1. Cơ quan nhà nước quy định cụ thể trách nhiệm, quyền hạn người dùng khi truy cập, đăng nhập các hệ thống thông tin, đảm bảo mỗi người dùng khi sử dụng hệ thống thông tin phải được cấp và sử dụng tài khoản truy cập với định danh duy nhất gắn với người dùng đó. Trường hợp sử dụng tài khoản dùng chung cho một nhóm người hay một đơn vị, bộ phận phải có cơ chế xác định các cá nhân có trách nhiệm quản lý tài khoản. Người dùng chỉ được truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình và có trách nhiệm bảo mật tài khoản truy cập được cấp.

2. Mật mã đăng nhập, truy cập hệ thống thông tin phải có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặc biệt như !, @, #, $, %,...) và phải được thay đổi theo thời gan nhất định.

3. Các cơ quan phải thực hiện việc ghi nhật ký (log) trên các thiết bị mạng máy tính, phần mềm ứng dụng, hệ điều hành, cơ sở dữ liệu nhằm đảm bảo các sự kiện quan trọng xảy ra trên hệ thống được ghi nhận và lưu giữ.

Điều 7. Đảm bảo an toàn các phần mềm ứng dụng

1. Trong quá trình đầu tư, thiết kế, xây dựng, nâng cấp, hủy bỏ (hoặc chuẩn bị thuê dịch vụ) phần mềm ứng dụng phải áp dụng các biện pháp quản lý và kỹ thuật đảm bảo các quy trình, kết quả xử lý của phần mềm phải trung thực (kết quả xử lý không bị can thiệp trái phép), kiểm soát lỗ hỏng bảo mật trong quá trình thiết kế, xây dựng phần mềm, kiểm soát phân quyền người dùng đăng nhập và kiểm soát các rủi ro mất an toàn thông tin khác có thể phát sinh, thực hiện nghiêm túc việc kiểm tra thử phần mềm trước khi đưa vào khai thác sử dụng.

2. Trong quá trình vận hành: Kiểm tra, giám sát việc tuân thủ các quy định về an toàn thông tin, an ninh thông tin đảm bảo cập nhật các lỗ hỏng bảo mật, áp dụng cơ chế sao lưu dự phòng, đảm bảo an toàn truy cập, đăng nhập hệ thống.

Điều 8. Bảo vệ bí mật nhà nước trong ứng dụng Công nghệ thông tin

1. Các văn bản có nội dung mật không được truyền trên mạng mà phải được quản lý chế độ mật theo quy định pháp luật hiện hành. Trường hợp đặc biệt, cần truyền thông tin mật trên mạng phải được Thủ trưởng cơ quan, đơn vị cho phép, trước khi truyền thông tin phải được mã hóa theo quy định của Luật Cơ yếu.

2. Các cơ quan, đơn vị phải bố trí máy vi tính riêng, không sử dụng máy tính kết nối Internet và các thiết bị di động thông minh để soạn thảo văn bản, lưu giữ thông tin có nội dung mật theo quy định. Các thiết bị viễn thông, máy tính được sử dụng để lưu giữ và truyền thông tin bí mật nhà nước phải được chứng nhận của cơ quan chức năng kiểm tra, kiểm định trước khi đưa vào sử dụng.

3. Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật, các cơ quan phải báo cáo cho cơ quan có thẩm quyền. Không được cho phép các công ty tư nhân hoặc cá nhân không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố.

Điều 9. Quản lý sự cố

Khi có sự cố hoặc nguy cơ mất an toàn thông tin, an ninh thông tin thì lãnh đơn vị phải chỉ đạo kịp thời, đồng thời phối hợp với cán bộ chuyên trách CNTT của Văn phòng HĐND & UBND, Phòng VH&TT huyện để khắc phục và hạn chế thiệt hại, báo cáo bằng văn bản cho cơ quan cấp trên trực tiếp quản lý và Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ.

Điều 10. Các hành vi bị nghiêm cấm

1. Xâm nhập, sửa đổi, xóa bỏ nội dung thông tin của cơ quan, cá nhân khác.

2. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin.

3. 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.

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

5. 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.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN, AN NINH THÔNG TIN

Điều 11. Trách nhiệm của các cơ quan

1. Thủ trưởng các cơ quan tổ chức thực hiện nghiêm túc các quy định tại Quy chế này và chịu trách nhiệm trước Chủ tịch Ủy ban nhân dân huyện trong công tác đảm bảo an toàn thông tin, an ninh thông tin của đơn vị mình.

2. Ban hành quy trình nội bộ về đảm bảo an toàn thông tin phù hợp với Quy chế này và các quy định của pháp luật.

3. Đưa nội dung thực hiện đảm bảo an toàn thông tin, an ninh thông tin vào kế hoạch ứng dụng công nghệ thông tin, thực hiện chương trình chuyển đổi số hàng năm của đơn vị.

4. Tuyên truyền, phổ biến Quy chế này và các quy định khác của pháp luật có liên quan về an toàn thông tin, an ninh thông tin trong phạm vi trách nhiệm và quyền hạn.

5. Phân công một cán bộ phụ trách đảm bảo an toàn thông tin, an ninh thông tin của đơn vị; tạo điều kiện để các cán bộ phụ trách an toàn thông tin, an ninh thông tin được học tập, nâng cao trình độ, đồng thời tạo điều kiện để cán bộ, công chức, viên chức và người lao động tham gia tập huấn kiến thức về an toàn thông tin, an ninh thông tin.

6. Thực hiện tốt việc phối hợp ứng cứu sự cố an toàn khi có nguy cơ mất an toàn thông tin, tạo điều kiện thuận lợi cho các cơ quan chức năng, tổ chức tham gia khắc phục sự cố và thực hiện đúng theo hướng dẫn.

7. Phối hợp với đoàn kiểm tra việc thực hiện đảm bảo an toàn thông tin, an ninh thông tin.

8. Thực hiện cam kết đảm bảo an ninh, an toàn, và bảo mật thông tin trong kết nối đến "Cơ sở dữ liệu Quốc gia về dân cư".

9. Báo cáo tình hình, kết quả thực hiện công tác đảm bảo an toàn thông tin, an ninh thông tin tại cơ quan về UBND huyện qua phòng VH&TT trước ngày 15 tháng 12 hàng năm để tổng hợp báo cáo Sở Thông tin và Truyền thông.

Điều 12. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các cơ quan

1. Trách nhiệm của cán bộ phụ trách an toàn thông tin, an ninh thông tin tại các cơ quan nhà nước:

a) Tham mưu lãnh đạo ban hành quy trình, biện pháp nhằm đảm bảo an toàn, an ninh thông tin; vận hành an toàn hệ thống thông tin của đơn vị theo nhiệm vụ được Thủ trưởng đơn vị phân công và theo các nội dung của Quy chế này.

b) Thực hiện giám sát, theo dõi việc tuân thủ thực hiện quy định về an toàn, an ninh thông tin tại đơn vị, kịp thời phát hiện các nguy cơ mất an toàn, an ninh thông tin để báo cáo, tham mưu lãnh đạo chỉ đạo thực hiện.

c) Phối hợp với các cơ quan, tổ chức, cá nhân liên quan trong việc kiểm tra, khắc phục sự cố mất an toàn, an ninh thông tin.

d) Tham gia các chương trình đào tạo, tập huấn chuyên môn, hội nghị về an toàn

thông tin, an ninh thông tin nhằm nâng cao nhận thức, năng lực chuyên môn, nghiệp vụ.

2. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các cơ quan nhà nước:

a) Thực hiện nghiêm các quy trình nội bộ của cơ quan, quy trình về an toàn, an ninh thông tin cũng như các quy định khác của pháp luật, nâng cao ý thức cảnh giác, trách nhiệm đảm bảo an toàn, an ninh thông tin tại đơn vị.

b) Khi phát hiện sự cố phải báo cáo ngay với cấp trên và bộ phận hoặc cán bộ phụ trách an toàn, an ninh thông tin để kịp thời ngăn chặn, xử lý.

c) Tham gia các chương trình đào tạo, tập huấn, hội nghị về an toàn, an ninh thông tin nhằm nâng cao nhận thức về an toàn, an ninh thông tin.

e) Nghiêm cấm mọi hành vi theo Điều 10 quy chế này.

f) Thực hiện cam kết đảm bảo an ninh, an toàn, và bảo mật thông tin trong kết nối đến "Cơ sở dữ liệu Quốc gia về dân cư".

Điều 13. Trách nhiệm của Phòng Văn hóa và Thông tin

1. Tham mưu Ủy ban nhân dân huyện về công tác đảm bảo an toàn, an ninh thông tin trên địa bàn.

2. Hàng năm, tham mưu xây dựng kế hoạch ứng dụng và phát triển công nghệ thông tin trong cơ quan nhà nước trên địa bàn huyện trong đó lòng ghép nội dung đảm bảo an toàn, an ninh thông tin và đưa tiêu chí an toàn, an ninh thông tin vào đánh giá mức độ hoàn thành nhiệm vụ các cơ quan.

3. Xây dựng Kế hoạch tập huấn và các hoạt động tuyên truyền đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn huyện.

4. Thực hiện việc tiếp nhận và xử lý các sự cố về an toàn, an ninh thông tin trên địa bàn huyện đồng thời tùy theo mức độ sự cố, phối hợp với các ngành chức năng liên quan hướng dẫn xử lý, ứng cứu các sự cố mất an toàn, an ninh thông tin.

5. Phối hợp với Công an và các cơ quan nhà nước có liên quan thành lập Đoàn kiểm tra an toàn, an ninh thông tin, tổ chức kiểm tra theo định kỳ hoặc kiểm tra đột xuất, kịp thời phát hiện và xử lý theo quy định pháp luật đối với các cơ quan, tổ chức, cá nhân có dấu hiệu, hành vi vi phạm an toàn thông tin.

Điều 14. Trách nhiệm Văn phòng HĐND & UBND huyện

1. Là đơn vị trực tiếp quản trị các hệ thống thông tin của huyện phải có trách nhiệm ban hành Quy trình nội bộ và thực hiện tốt công tác đảm bảo an toàn thông tin theo các nội dung của Quy chế này, các tiêu chuẩn quốc gia về an toàn thông tin.

2. Cử cán bộ quản trị mạng phụ trách an toàn, an ninh thông tin của huyện.

Chương IV
KIỂM TRA, KHEN THƯỞNG VÀ XỬ LÝ VI PHẠM AN TOÀN, AN NINH THÔNG TIN

Điều 15. Kiểm tra

1. Phòng Văn hóa và Thông tin chủ trì, phối hợp với các cơ quan nhà nước có liên

quan tiến hành kiểm tra công tác đảm bảo an toàn thông tin định kỳ hoặc đột xuất đối với các cơ quan nhà nước trên địa bàn huyện.

2. Công an huyện chủ, phối hợp với các cơ quan nhà nước có liên quan tiến hành kiểm tra công tác đảm bảo an ninh thông tin định kỳ hoặc đột xuất đối với các cơ quan nhà nước trên địa bàn huyện.

Điều 16. Khen thưởng, xử lý vi phạm

1. Hàng năm trên cơ sở công tác, kiểm tra và báo cáo công tác an toàn, an ninh thông tin của các cơ quan nhà nước để tổng hợp, báo cáo và đề xuất Ủy ban nhân dân huyện xem xét khen thưởng các cá nhân, đơn vị theo quy định hiện hành.

2. Tổ chức, cá nhân có hành vi vi phạm Quy chế này, tùy theo tính chất, mức độ vi phạm bị xử lý kỷ luật theo quy định hiện hành.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 17. Điều khoản thi hành

1. Thủ trưởng cơ quan, ban, ngành, đoàn thể huyện, Chủ tịch Ủy ban nhân dân xã, thị trấn và các đơn vị có liên quan chịu trách nhiệm tổ chức triển khai thực hiện Quy chế này.

2. Trong quá trình thực hiện, nếu có những vấn đề cần sửa đổi, bổ sung, đề nghị các cơ quan gửi về phòng Văn hóa và Thông tin để tổng hợp, báo cáo Ủy ban nhân dân huyện xem xét, quyết định./.