UBND TỈNH KHÁNH HÒA
BAN QUẢN LÝ DỰ ÁN PHÁT TRIỂN TỈNH KHÁNH HÒA

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

QUY CHẾ

Đảm bảo an toàn thông tin cho Trang thông tin điện tử tổng hợp Ban Quản lý dự án Phát triển tỉnh Khánh Hòa

(Ban hành kèm theo Quyết định số: 576 /QĐ-BQL ngày 07 tháng 11 năm 2025 của Ban Quản lý dự án Phát triển tỉnh Khánh Hòa)

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Quy chế này quy định các nội dung về bảo đảm an toàn thông tin cho Trang thông tin điện tử tổng hợp của Ban Quản lý dự án Phát triển tỉnh Khánh Hòa có địa chỉ: https://kdpm.khanhhoa.gov.vn hoặc https://kdpm.vn

2. Quy chế này được áp dụng đối với các tổ chức, cá nhân liên quan đến an toàn thông tin cho Trang thông tin điện tử tổng hợp của Ban Quản lý dự án Phát triển tỉnh Khánh Hòa.

Điều 2. Mục đích, nguyên tắc quản lý trang thông tin điện tử

1. Việc áp dụng Quy định này nhằm phòng ngừa, ngăn chặn nguy cơ gây mất an toàn thông tin và đảm bảo an ninh thông tin trong quá trình quản lý và sử dụng Trang thông tin điện tử tổng hợp của Ban Quản lý dự án Phát triển tỉnh Khánh Hòa.

2. Các hoạt động ứng dụng công nghệ thông tin phải tuân theo các quy định tại Nghị định số 147/2024/NĐ-CP ngày 09/11/2024 của Chính phủ về Quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng.

3. Nội dung thông tin cung cấp trên Trang Thông tin điện tử thực hiện theo quy định tại Điều 4 Nghị định số 42/2022/NĐ-CP ngày 24/6 /2022 của Chính phủ quy định về việc cung cấp thông tin và dịch vụ công trực tuyến của cơ quan nhà nước trên môi trường mạng và các quy định hiện hành.

4. Thông tin cung cấp trên Trang Thông tin điện tử phải đúng với quan điểm, chủ trương, đường lối của Đảng, chính sách và pháp luật của Nhà nước; phục vụ kịp thời công tác chỉ đạo điều hành, tuyên truyền của cơ quan nhà nước và nhu cầu tìm kiếm, khai thác thông tin của các tổ chức, cá nhân.

5. Thông tin cung cấp trên Trang Thông tin điện tử phải tuân thủ các quy định của pháp luật về bảo vệ bí mật nhà nước, báo chí, sở hữu trí tuệ và quản lý thông tin trên Internet.

6. Khi đăng tải, trích dẫn, sử dụng lại thông tin từ các nguồn tin chính thức từ Cổng Thông tin điện tử phải ghi chính xác nguồn tin, tên tác giả hoặc tên cơ quan của nguồn tin chính thức theo quy định tại Điều 28 Nghị định số 147/2024/NĐ-CP ngày 09 tháng 11 năm 2024 của Chính phủ về quản lý, cung

cấp, sử dụng dịch vụ Internet và thông tin trên mạng.

7. Thông tin đăng tải trên Trang Thông tin điện tử là thông tin chính thống của cơ quan nhà nước trên môi trường mạng.

8. Các thông tin do cơ quan nhà nước và tổ chức, cá nhân cung cấp, trước khi đưa lên Trang Thông tin điện tử phải được Ban Biên tập Trang Thông tin điện tử kiểm duyệt và phải chịu trách nhiệm theo quy định của pháp luật về các thông tin cung cấp trên Trang Thông tin điện tử.

Điều 3. Quản lý nội dung thông tin

3.1. Trang thông tin điện tử:

- Có quy trình quản lý thông tin công cộng: Xác định phạm vi nguồn thông tin khai thác, cơ chế quản lý, kiểm tra thông tin trước và sau khi đăng tải;

- Có cơ chế kiểm soát nguồn tin, đảm bảo thông tin tổng hợp đăng tải phải chính xác theo đúng thông tin nguồn;

- Có cơ chế phối hợp để có thể loại bỏ ngay nội dung vi phạm theo quy định tại Điều 8 Luật An ninh mạng chậm nhất sau 03 giờ kể từ khi tự phát hiện hoặc có yêu cầu của Bộ Thông tin và Truyền thông hoặc cơ quan cấp phép (bằng văn bản, điện thoại, email).

3.2. Quy trình quản lý thông tin công cộng:

Bảo đảm chỉ lựa chọn thông tin từ các nguồn tin có nội dung phù hợp với lợi ích quốc gia, lợi ích của xã hội, lợi ích hợp pháp của tổ chức, cá nhân. Rà soát, kiểm tra nội dung tin bài trước khi đăng tải, phát hiện và loại bỏ ngay thông tin không còn tồn tại ở nguồn tin, những thông tin công cộng có nội dung vi phạm Điều 8 Luật An ninh mạng.

Đồng thời, thực hiện nghiêm việc tổng hợp thông tin tuân theo quy định tại Mục 2 Chương III và các quy định có liên quan tại Nghị định số 147/2024/NĐ-CP của Chính phủ: Quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng và các quy định có liên quan về báo chí.

3.3 Quy trình tiếp nhận, kiểm duyệt và xử lý thông tin cụ thể như sau:

Bước 1. Tiếp nhận và xử lý thông tin

Ban Biên tập tiếp nhận thông tin đăng tải do các đơn vị, cá nhân gửi về qua email hoặc các kênh khác.

Bước 2: Xác thực thông tin

- Trưởng Ban Biên tập hoặc thành viên được ủy quyền kiểm tra, xác định rõ nguồn gốc, mục đích thông tin và báo cáo để quyết định đăng tải.

- Trường hợp thông tin chưa đầy đủ, chưa rõ ràng, chưa chính xác người được phân công xác thực có trách nhiệm trao đổi, làm rõ và yêu cầu bổ sung thông tin.

Bước 3: Tổng hợp và biên tập thông tin

- Ban Biên tập rà soát, chỉnh sửa bố cục, nội dung các bài viết trước khi đăng.

Bước 4: Đăng tải thông tin

- Trưởng Ban Biên tập hoặc thành viên Ban Biên tập được ủy quyền kiểm tra lại tính chính xác của thông tin lần cuối và chuyển cho Thư ký/Quản trị viên để đăng tải.

- Thông tin gửi đăng tải cần ghi rõ tên các tác giả (đồng tác giả, nếu có), tiêu đề bài viết và đề mục đăng tải trên Trang thông tin điện tử.

3.4. Cơ chế kiểm soát nguồn tin:

a) Xác thực nguồn tin

- Kiểm tra nguồn gốc và độ tin cậy của thông tin.
- Đối chiếu với các nguồn uy tín khác để đảm bảo tính chính xác.

b) Kiểm duyệt nội dung

- Kiểm tra tính chính xác và tính logic của nội dung.
- Đánh giá nội dung dựa trên các tiêu chí như tính khách quan, trung thực, và tuân thủ pháp luật.

c) Phát hiện và xử lý thông tin sai lệch:

- Lọc thông tin dựa trên các tiêu chí:

+ *Nguồn tin*: Kiểm tra độ tin cậy của nguồn, xác minh thông tin liên hệ.

+ *Nội dung*: Xác minh tính logic, dẫn chứng, sự kiện và tính nhất quán với các thông tin khác.

+ *Ngữ phong*: Nhận diện dấu hiệu của thông tin giả mạo như: ngôn ngữ kích động, quá khích, thiếu bằng chứng.

- Xác minh và đánh giá:

+ *Kiểm tra chéo thông tin*: So sánh thông tin từ nhiều nguồn khác nhau để xác minh tính chính xác. Phối hợp với các cơ quan kiểm chứng thông tin và các cơ quan nhà nước để tăng cường hiệu quả.

+ *Tìm kiếm bằng chứng*: Sử dụng bằng chứng trực quan, tài liệu, báo cáo để hỗ trợ hoặc bác bỏ thông tin.

+ *Đánh giá mức độ ảnh hưởng:* Xác định mức độ ảnh hưởng của thông tin sai lệch đến dư luận và xã hội.

- Báo cáo và xử lý sai lệch:

+ *Báo cáo nội bộ:* Thông báo ngay cho các bộ phận liên quan để quyết định phương thức xử lý.

+ *Xử lý nhanh chóng:*

- Gỡ bỏ các nội dung sai lệch.
- Chỉnh sửa thông tin.
- Cảnh báo người dùng về thông tin không chính xác.

+ *Phản hồi người dùng:* Đảm bảo phản hồi rõ ràng, minh bạch với người dùng khi có thắc mắc hoặc ý kiến.

+ *Xây dựng thông điệp chính thức:* Đưa ra thông điệp chính thức để làm rõ sự thật và giảm thiểu tác động của thông tin sai lệch.

+ *Cập nhật cơ sở dữ liệu:* Lưu trữ thông tin về các trường hợp sai lệch đã được xác minh để sử dụng trong tương lai.

3.5. Cơ chế phối hợp để có thể loại bỏ ngay nội dung vi phạm:

Bước 1: Cơ quan nhà nước có thẩm quyền gửi yêu cầu đến Ban QLDA thông qua nhân sự đầu mối tiếp nhận thông tin của Ban QLDA bằng các phương thức cụ thể:

- Tên tổ chức: Ban Quản lý dự án Phát triển tỉnh Khánh Hòa
- Địa chỉ trụ sở: 37 Tô Vĩnh Diện, Phường Tây Nha Trang, tỉnh Khánh Hòa
- Họ tên (người đầu mối liên lạc): ông Nguyễn Thanh Hiến
- Số điện thoại liên lạc: 0258 3562204
- E-mail: kdpm@khanhhoa.gov.vn hoặc khanhhoadpmu@gmail.com

Bước 2: Xử lý nội bộ

- Trưởng Ban biên tập sẽ phân công cho các thành viên Ban biên tập rà soát yêu cầu từ cơ quan chức năng.
- Chuyển yêu cầu đến bộ phận hoặc cá nhân có thẩm quyền phụ trách trong nội bộ tổ chức để xử lý.
- Tổ chức cuộc họp (nếu cần) để xác định cách giải quyết và thời hạn xử lý yêu cầu.
- Phân công trách nhiệm cụ thể cho từng cá nhân hoặc phòng chuyên môn có liên quan.

Bước 3: Biện pháp xử lý hoặc kết quả

- Cung cấp thông tin, tài liệu theo yêu cầu của cơ quan nhà nước có thẩm quyền.
- Đề xuất giải pháp hoặc biện pháp khắc phục (nếu liên quan đến vi phạm, sự cố).
- Xây dựng báo cáo chi tiết về cách thức giải quyết và kết quả đạt được.

Bước 4: Phản hồi cho cơ quan quản lý nhà nước có thẩm quyền

- Tổng hợp các tài liệu, báo cáo, biên bản làm việc hoặc kết quả xử lý để gửi lại cho cơ quan nhà nước theo yêu cầu.
- Đảm bảo phản hồi đúng thời hạn quy định.
- Xác nhận việc tiếp nhận thông tin phản hồi và giữ liên lạc để xử lý các vấn đề phát sinh (nếu có).

Điều 4. Yêu cầu kỹ thuật cho trang thông tin điện tử

Trang thông tin điện tử thực hiện bảo đảm an toàn hệ thống thông tin theo cấp độ quy định tại Nghị định số 85/2016/NĐ-CP về bảo đảm an toàn hệ thống thông tin theo cấp độ và Thông tư số 12/2022/TT-BTTTT về quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; có giải pháp hiệu quả chống lại các tấn công gây mất an toàn thông tin mạng Trang thông tin điện tử; có phương án dự phòng khắc phục sự cố bảo đảm Trang thông tin điện tử hoạt động liên tục ở mức tối đa.

- Trang thông tin điện tử được lưu trữ tại 01 máy chủ đặt tại trung tâm dữ liệu tại Việt Nam, hệ thống lưu trữ tối thiểu 90 ngày đối với nội dung thông tin tổng hợp kể từ thời điểm đăng tải; lưu trữ tối thiểu 02 năm đối với nhật ký xử lý thông tin được đăng tải.

- Trang thông tin điện tử có cơ chế tiếp nhận và xử lý cảnh báo thông tin vi phạm từ người sử dụng thông qua kênh hỗ trợ kỹ thuật của đơn vị vận hành hoặc/và đơn vị quản lý hoặc/và khi các bên nhận được cảnh báo từ cơ chế tự động phát hiện, cảnh báo đã được thiết lập trên hệ thống.

4.1. Cơ chế tiếp nhận và xử lý cảnh báo như sau:

- Trang thông tin điện tử có cơ chế tự động phát hiện, cảnh báo và ngăn chặn truy nhập bất hợp pháp, các hình thức tấn công trên môi trường mạng và tuân theo những tiêu chuẩn đảm bảo an toàn thông tin thông qua phần mềm bảo mật ESET PROTECT Server Security, cụ thể:

- Hệ thống giám sát và cảnh báo an ninh (Security Information and Event Management - SIEM): Sử dụng các công cụ giám sát và phân tích log, đặt ra các ngưỡng cảnh báo cho các hoạt động bất thường như:

+ Tăng đột biến lưu lượng truy cập.

+ Lỗi đăng nhập nhiều lần.

+ Thao tác bất thường trên hệ thống (ví dụ: xóa dữ liệu hàng loạt).

Khi phát hiện các hoạt động nghi ngờ, hệ thống sẽ gửi cảnh báo đến các quản trị viên qua email, SMS, hoặc thông qua các công cụ giám sát như dashboard hoặc công cụ quản lý sự cố, giúp phản hồi kịp thời.

- Quy trình xử lý cảnh báo:

+ Xác định mức độ nghiêm trọng của cảnh báo.

+ Phân tích nguyên nhân.

+ Thực hiện các hành động khắc phục (ví dụ: chặn IP, reset mật khẩu, kiểm tra hệ thống).

+ Ghi lại quá trình xử lý để phục vụ cho việc đánh giá và cải tiến hệ thống.

4.2. Các giải pháp bảo mật

- Phát hiện:

+ *Tường lửa (Firewall):* Chỉ cho phép các địa chỉ IP và cổng cụ thể truy cập vào hệ thống. Tường lửa Windows có thể được cấu hình để chặn truy cập từ các địa chỉ không đáng tin cậy Chặn các kết nối đến từ các địa chỉ IP đáng ngờ, các cổng không cần thiết.

+ *WAF:* Phát hiện và ngăn chặn các cuộc tấn công vào ứng dụng web như SQL Injection, XSS.

+ *Hệ thống phát hiện xâm nhập (IDS):* Phân tích lưu lượng mạng để tìm kiếm các dấu hiệu của cuộc tấn công và gửi cảnh báo. Trong khi đó, IPS có thể ngăn chặn ngay lập tức các hành động xâm nhập.

+ *Phần mềm diệt virus và phần mềm chống mã độc (Anti-Malware):* giúp

phát hiện, cách ly và loại bỏ các phần mềm độc hại có thể đã xâm nhập vào hệ thống.

- Cảnh báo:

+ *Email:* Gửi thông báo đến đội ngũ quản trị viên khi có sự cố xảy ra.

+ *SMS*: Gửi tin nhắn đến điện thoại di động của người quản trị.

+ *Công cụ giám sát*: Hiển thị cảnh báo trên giao diện quản trị.

- Ngăn chặn:

+ *Chặn IP:* Ngăn chặn truy cập từ các địa chỉ IP đáng ngờ.

+ *Khóa tài khoản:* Khóa tài khoản người dùng khi phát hiện hoạt động bất thường.

+ *Cấu hình xác thực và phân quyền:* Xác thực Windows Authentication hoặc Basic Authentication: Sử dụng Windows Authentication cho các ứng dụng nội bộ để tận dụng cơ chế xác thực mạnh mẽ của hệ thống bằng cách yêu cầu người dùng xác minh danh tính qua nhiều phương thức (mật khẩu, tin nhắn điện thoại).

- Phân quyền người dùng: Thiết lập quyền truy cập đúng mức cho các tài khoản hệ thống và ứng dụng, chỉ cung cấp quyền tối thiểu cần thiết (Principle of Least Privilege), yêu cầu người dùng thay đổi mật khẩu định kỳ. Cấp quyền truy cập cho người dùng dựa trên vai trò và nhiệm vụ của họ. Vô hiệu hóa quyền "anonymous authentication" nếu không cần thiết, để ngăn chặn các truy cập không xác định.

+ *Giới hạn quyền truy cập vào thư mục và file*: Phân quyền file và thư mục: Thiết lập quyền truy cập trên file hệ thống IIS chỉ có những tài khoản cần thiết mới có thể truy cập, chỉnh sửa. Chỉ cấp cho người dùng quyền truy cập tối thiểu cần thiết để thực hiện công việc. Hệ thống có thể được cấu hình để giới hạn số lần đăng nhập sai, giúp ngăn chặn tấn công brute force.

+ *Cấu hình HTTPS:* Cài đặt SSL/TLS: Các kết nối đến máy chủ web được mã hóa thông qua HTTPS. Sử dụng TLS mới nhất: Máy chủ hỗ trợ các phiên bản TLS an toàn (như TLS 1.2, TLS 1.3) giúp tăng cường bảo mật, ngăn ngừa các cuộc tấn công man-in-the-middle. Quét lỗ hổng SSL/TLS thường xuyên để phát hiện và khắc phục các lỗ hổng tiềm ẩn trong cấu hình SSL/TLS.

+ *Cấu hình tường lửa (Firewall):* Cấu hình tường lửa chỉ cho phép các cổng và địa chỉ IP cụ thể truy cập vào máy chủ.

+ *Web Application Firewall (WAF*): Cài đặt WAF để lọc và giám sát lưu lượng HTTP nhằm bảo vệ ứng dụng web khỏi các lỗ hổng như SQL Injection, Cross-Site Scripting (XSS), và tấn công DDoS.

+ *Cấu hình ngăn chặn tấn công DDoS và hạn chế kết nối:* Sử dụng dịch vụ bảo vệ DDoS chuyên nghiệp để giảm thiểu tác động của các cuộc tấn công. Hạn chế tốc độ kết nối: Đặt giới hạn số lượng kết nối đồng thời từ một địa chỉ IP. Cấu hình rate limiting: Hạn chế số lượng yêu cầu đến từ một nguồn trong một khoảng thời gian nhất định.

+ *Cập nhật các bản vá lỗi hệ thống thường xuyên.*

+ *Logging và giám sát*: Cấu hình logging, bật tính năng log của IIS để ghi lại toàn bộ các yêu cầu truy cập, bao gồm thông tin về địa chỉ IP, loại yêu cầu, trạng thái HTTP. Tích hợp với SIEM: Sử dụng hệ thống giám sát tập trung (SIEM) để theo dõi log từ IIS và các dịch vụ khác trên hệ thống. Lưu trữ log trong một khoảng thời gian đủ dài để phục vụ cho việc điều tra khi cần thiết. Sử dụng các công cụ phân tích log để tìm kiếm các hành vi bất thường. Tích hợp với SIEM và các hệ thống giám sát khác, tạo một hệ thống giám sát thống nhất để theo dõi toàn bộ môi trường.

+ *Bảo mật ứng dụng web*: Giới hạn upload file, giới hạn kích thước, định dạng file.

+ *Anti-Malware:* Cài đặt phần mềm diệt virus. Kiểm tra mã nguồn phát hiện các lỗ hổng bảo mật; quét lỗ hổng web định kỳ để phát hiện các lỗ hổng mới.

- Hệ thống có phương án dự phòng bảo đảm duy trì hoạt động an toàn, liên tục và khắc phục khi có sự cố xảy ra, trừ những trường hợp bất khả kháng theo quy định của pháp luật.

4.3. Phương án dự phòng:

Trang thông tin điện tử Ban QLDA có hỗ trợ cơ chế sao lưu dữ liệu tự động hàng ngày, dữ liệu sao lưu được lưu trữ trên hạ tầng vStorage tại Việt Nam (Dịch vụ lưu trữ đám mây Object Storage), dữ liệu sao lưu được quản lý bởi đơn vị vận hành máy chủ nhằm đảm bảo nhanh chóng đưa hệ thống hoạt động trở lại trong trường hợp có sự cố xảy ra. Cho phép lưu trữ nội dung, dữ liệu lớn dần theo thời gian sử dụng, việc lưu trữ có thể thực hiện trong các cơ sở dữ liệu, thư mục tệp tin hệ thống.

- Các dữ liệu cần sao lưu:

+ Dữ liệu cấu hình hệ thống (Quản lý người sử dụng; cấu hình thiết lập kênh thông tin…).

+ Cơ sở dữ liệu lưu trữ nội dung.

+ Các dữ liệu liên quan khác.

- Các dữ liệu sao lưu luôn trong tình trạng sẵn sàng bàn giao cho Ban QLDA khi được yêu cầu.

- Nơi lưu trữ dữ liệu dự phòng: Máy chủ sao lưu (Backup Server), các bản sao dữ liệu sẽ được lưu trữ trên một máy chủ sao lưu riêng biệt hoặc thiết bị lưu trữ ngoại vi.

- Phương thức sao lưu: Sao lưu toàn bộ, sao lưu tất cả dữ liệu vào một khoảng thời gian nhất định giúp khôi phục toàn bộ hệ thống một cách dễ dàng. Sau đó sao lưu các thay đổi kể từ lần sao lưu toàn bộ gần nhất.

- Người thực hiện: nhân viên quản trị trang thông tin điện tử (với sự hỗ trợ của cán bộ kỹ thuật của Công ty cổ phần SweetSoft) thực hiện công tác sao lưu, chịu trách nhiệm quản lý, theo dõi và bảo trì hệ thống sao lưu, bao gồm cả việc kiểm tra tính toàn vẹn của các bản sao lưu.

- Tần suất sao lưu: Hàng tuần hoặc hàng tháng, tần suất sao lưu phụ thuộc vào mức độ thay đổi dữ liệu và yêu cầu của hệ thống.

- Kiểm tra và khôi phục: Định kỳ, nhân viên quản trị trang thông tin điện tử (với sự hỗ trợ của cán bộ kỹ thuật của Công ty cổ phần SweetSoft) kiểm tra tính toàn vẹn của dữ liệu sao lưu để đảm bảo rằng bản sao lưu có thể sử dụng được khi cần. Thực hiện các cuộc thử nghiệm khôi phục để đảm bảo rằng quá trình sao lưu hoạt động hiệu quả và có thể khôi phục dữ liệu khi có sự cố.

Điều 5. Quản lý, vận hành hoạt động Trang Thông tin điện tử

1. Giao phòng Hành chính Tổng hợp:

- Chịu trách nhiệm quản lý, quản trị, vận hành hoạt động Trang Thông tin điện tử Ban QLDA theo quy định của pháp luật; bố trí viên chứcc có trình độ, kỹ năng công nghệ thông tin, có khả năng quản trị nội dung và truyền thông số làm đầu mối thực hiện quản lý, vận hành Trang Thông tin điện tử Ban QLDA theo các quy định hiện hành.

- Chịu trách nhiệm phối hợp với đơn vị cung cấp dịch vụ tư vấn đảm bảo an toàn thông tin, dữ liệu trên Trang Thông tin điện tử; thực hiện quản lý, bảo mật thông tin tài khoản, sử dụng tài khoản (Users) và mật khẩu (Password) được cấp đúng theo quy định; thường xuyên kiểm tra, rà soát các chuyên mục thông tin, cập nhật thông tin trên Trang Thông tin điện tử đầy đủ, kịp thời.

- Chủ trì, phối hợp với các phòng chuyên môn triển khai việc thực hiện Quy chế này.

2. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc cần sửa đổi, bổ sung thì đề xuất lãnh đạo Ban xem xét, quyết định./.