

KẾ HOẠCH

Triển khai thực hiện Quyết định số 515/QĐ-TTg ngày 30 tháng 3 năm 2026 của Thủ tướng Chính phủ phê duyệt Đề án “Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia”

Thực hiện Kế hoạch số 10442/KH-UBND ngày 19/8/2026 của Ủy ban nhân dân tỉnh Khánh Hòa về Triển khai thực hiện Quyết định số 515/QĐ-TTg ngày 30 tháng 3 năm 2026 của Thủ tướng Chính phủ phê duyệt Đề án “Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia” trên địa bàn tỉnh Khánh Hòa;

Căn cứ chức năng, nhiệm vụ và tình hình thực tế của đơn vị, Ban Quản lý Vườn quốc gia Núi Chúa - Phước Bình xây dựng Kế hoạch thực hiện với các nội dung cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Cụ thể hóa đầy đủ, đồng bộ các quan điểm, mục tiêu, nhiệm vụ và giải pháp của Quyết định số 515/QĐ-TTg và Kế hoạch của Ủy ban nhân dân tỉnh Khánh Hòa phù hợp với chức năng, nhiệm vụ và điều kiện thực tế của Ban Quản lý Vườn quốc gia Núi Chúa - Phước Bình.

- Nâng cao nhận thức, trách nhiệm của lãnh đạo, viên chức, người lao động và các cá nhân có liên quan trong việc bảo đảm an toàn, an ninh mạng; chủ động phòng ngừa, phát hiện và xử lý các nguy cơ mất an toàn thông tin trong quá trình thực hiện nhiệm vụ.

- Gắn nhiệm vụ bảo vệ an ninh mạng với việc ứng dụng khoa học, công nghệ, chuyển đổi số trong hoạt động quản lý, bảo vệ rừng, bảo tồn thiên nhiên, nghiên cứu khoa học, quản lý tài nguyên, quản lý hành chính và các hoạt động chuyên môn của Ban Quản lý.

2. Yêu cầu

- Bám sát nội dung, lộ trình của Quyết định số 515/QĐ-TTg và Kế hoạch của Ủy ban nhân dân tỉnh Khánh Hòa; phân công nhiệm vụ theo nguyên tắc “rõ người, rõ việc, rõ trách nhiệm, rõ thời gian, rõ sản phẩm, rõ kết quả”, bảo đảm thiết thực, khả thi, không hình thức, không trùng lặp.

- Bảo đảm an ninh mạng đối với hệ thống thông tin, thiết bị, tài khoản và dữ liệu thuộc phạm vi quản lý của Ban Quản lý; chủ động phòng ngừa, phát hiện, xử lý và khắc phục các nguy cơ, sự cố.

- Kết hợp chặt chẽ giữa việc kiện toàn đầu mối, nâng cao nhận thức, đào tạo, tập huấn với việc bảo đảm hạ tầng, trang thiết bị, quy trình quản lý, sử dụng và bảo vệ hệ thống thông tin, dữ liệu.

- Việc triển khai phải tuân thủ quy định của pháp luật về an ninh mạng, bảo vệ bí mật nhà nước, an ninh dữ liệu, đầu tư công, ngân sách nhà nước, đấu thầu và các quy định có liên quan; bảo đảm tiết kiệm, hiệu quả, tránh đầu tư phân tán, chồng chéo.

II. MỤC TIÊU

1. Mục tiêu tổng quát

Nâng cao năng lực bảo đảm an ninh mạng của Ban Quản lý; chủ động phòng ngừa, phát hiện, ngăn chặn và xử lý hiệu quả các nguy cơ, thách thức, sự cố và hành vi vi phạm pháp luật trên không gian mạng; bảo vệ an toàn hệ thống thông tin, dữ liệu và hoạt động của đơn vị, góp phần thực hiện mục tiêu chung của tỉnh.

2. Mục tiêu cụ thể

a) Xác định rõ lãnh đạo phụ trách, đầu mối và lực lượng thực hiện nhiệm vụ bảo vệ an ninh mạng tại Ban Quản lý.

b) Rà soát, xác định các hệ thống thông tin, cơ sở dữ liệu, thiết bị, tài khoản và dữ liệu thuộc phạm vi quản lý của Ban Quản lý; thực hiện các biện pháp bảo đảm an ninh mạng theo quy định và hướng dẫn của cơ quan có thẩm quyền.

c) 100% viên chức, người lao động được phổ biến, cập nhật kiến thức và kỹ năng cơ bản về an toàn, an ninh mạng theo lộ trình của tỉnh.

d) Hằng năm tham gia ít nhất 01 hoạt động tập huấn, diễn tập hoặc thực hành xử lý tình huống an ninh mạng theo kế hoạch của tỉnh và phù hợp với phạm vi quản lý của Ban Quản lý

đ) Định kỳ kiểm tra, rà soát máy tính, thiết bị, tài khoản và các điểm có nguy cơ mất an toàn; kịp thời khắc phục các điểm yếu được phát hiện.

e) Thực hiện chế độ thông tin, báo cáo; báo cáo kịp thời các sự cố, nguy cơ nghiêm trọng về Công an tỉnh để phối hợp xử lý theo quy định.

f) Tham gia thiết lập cơ chế chia sẻ thông tin, cảnh báo sớm và điều phối ứng phó sự cố 24/7 với Công an tỉnh sau khi Trung tâm giám sát an ninh mạng (SOC) của tỉnh xây dựng và vận hành.

III. NHIỆM VỤ, GIẢI PHÁP

1. Hoàn thiện cơ chế, chính sách và quy trình phối hợp bảo đảm an ninh mạng

- Lồng ghép yêu cầu bảo đảm an ninh mạng trong các chương trình, kế hoạch, đề án, dự án ứng dụng công nghệ thông tin, chuyển đổi số, xây dựng cơ sở dữ liệu và đầu tư, mua sắm thiết bị công nghệ thông tin của Ban Quản lý.

- Hoàn thiện chế độ báo cáo, thống kê, kiểm tra, giám sát và đánh giá kết quả thực hiện; gắn trách nhiệm của người đứng đầu với tình hình bảo đảm an ninh mạng tại đơn vị.

2. Kiện toàn tổ chức, xây dựng lực lượng bảo vệ an ninh mạng

- Phân công lãnh đạo Ban Quản lý phụ trách công tác bảo đảm an ninh mạng.

- Phân công cán bộ làm đầu mối thực hiện, theo dõi, tham mưu công tác an ninh mạng của Ban quản lý phù hợp với vị trí việc làm và điều kiện nhân lực thực tế.

- Các phòng chuyên môn và đơn vị trực thuộc xác định viên chức phối hợp thực hiện nhiệm vụ khi có yêu cầu.

- Thường xuyên cập nhật thông tin liên hệ của đầu mối để phục vụ tiếp nhận cảnh báo, trao đổi thông tin và xử lý sự cố.

3. Đào tạo, bồi dưỡng và phát triển nguồn nhân lực an ninh mạng

- Khảo sát nhu cầu, đánh giá hiện trạng năng lực và xác định nhu cầu đào tạo, bồi dưỡng an ninh mạng của viên chức, người lao động thuộc Ban.

- Cử lãnh đạo và viên chức được giao nhiệm vụ liên quan đến công nghệ thông tin, an ninh mạng tham gia các chương trình đào tạo, bồi dưỡng do tỉnh và cơ quan có thẩm quyền tổ chức.

- Tổ chức hoặc tham gia đào tạo kiến thức, kỹ năng an ninh mạng, an ninh dữ liệu cho viên chức, người lao động theo chương trình, tài liệu và lộ trình của cấp có thẩm quyền.

- Phổ biến các phương thức, thủ đoạn lừa đảo, tấn công mạng; hướng dẫn kỹ năng bảo vệ tài khoản, thiết bị và dữ liệu.

4. Tổ chức huấn luyện, diễn tập và nâng cao năng lực ứng phó

- Hằng năm tham gia ít nhất 01 cuộc diễn tập chuyên đề phù hợp với phạm vi quản lý của Ban Quản lý theo yêu cầu của Kế hoạch tỉnh.

- Nội dung diễn tập tập trung vào các tình huống phù hợp với điều kiện thực tế của đơn vị như: mất quyền kiểm soát tài khoản; mã độc; mất dữ liệu; lộ lọt dữ liệu; thiết bị bị xâm nhập; mất thiết bị chứa dữ liệu; hệ thống thông tin bị gián đoạn.

- Tham gia các cuộc diễn tập cấp tỉnh khi được triệu tập hoặc yêu cầu.

- Sau diễn tập tổ chức đánh giá, rút kinh nghiệm và bổ sung, hoàn thiện phương án xử lý sự cố.

5. Đầu tư hạ tầng, trang thiết bị và nâng cao năng lực tự chủ công nghệ

- Bố trí đầu mối, nhân lực, kinh phí, trang thiết bị trong khả năng và theo phân cấp để thực hiện nhiệm vụ bảo đảm an ninh mạng.

- Hằng năm căn cứ nhiệm vụ được giao, nhu cầu thực tế và khả năng cân đối nguồn lực, lập dự toán kinh phí thực hiện các nhiệm vụ bảo đảm an ninh mạng, đào tạo, tập huấn, diễn tập, kiểm tra, bảo trì, nâng cấp và bảo đảm an toàn hệ thống thông tin.

- Việc quản lý, sử dụng kinh phí, mua sắm, thuê dịch vụ, đầu tư và quản lý tài sản thực hiện theo quy định hiện hành, bảo đảm công khai, minh bạch, tiết kiệm, hiệu quả và không trùng lặp.

6. Tuyên truyền, phổ biến kiến thức, nâng cao nhận thức và kỹ năng an ninh mạng

- Lồng ghép nội dung tuyên truyền, phổ biến kiến thức, kỹ năng an ninh mạng trong các cuộc họp, hội nghị, sinh hoạt chuyên môn, tập huấn nghiệp vụ và các hoạt động phù hợp của đơn vị; sử dụng các tài liệu, nội dung cảnh báo, khuyến cáo về an ninh mạng do cơ quan có thẩm quyền cung cấp để phổ biến đến viên chức, người lao động.

- Đăng ký tham gia các khóa học trực tuyến, mô hình “Bình dân học vụ số”, chuyên mục, video, infographic, bộ công cụ tự kiểm tra và cảnh báo; chú trọng phòng, chống lừa đảo trên không gian mạng.

- Tăng cường tuyên truyền trách nhiệm của người đứng đầu, viên chức, người lao động và doanh nghiệp trong quản lý tài khoản, dữ liệu, thiết bị, bí mật nhà nước và sử dụng an toàn các nền tảng số.

(Đính kèm Phụ lục Danh mục các nhiệm vụ triển khai)

IV. KINH PHÍ THỰC HIỆN

Kinh phí thực hiện Kế hoạch được bố trí từ nguồn ngân sách nhà nước cấp hàng năm cho hoạt động thường xuyên của đơn vị và các nguồn hợp pháp khác theo quy định.

V. TỔ CHỨC THỰC HIỆN

1. Phòng Hành chính - Tổ chức

Tham mưu đề xuất bố trí đầu mối, nhân lực, kinh phí, trang thiết bị và phối hợp với các phòng chuyên môn, đơn vị trực thuộc tổ chức triển khai đầy đủ các biện pháp bảo đảm an ninh mạng theo cấp độ.

Hằng năm, tham mưu cử viên chức tham gia các chương trình đào tạo, tập huấn, diễn tập về an toàn thông tin, an ninh mạng khi được cơ quan cấp trên triệu tập hoặc yêu cầu.

Phối hợp với các phòng chuyên môn, đơn vị trực thuộc tổ chức triển khai thực hiện Kế hoạch này; chịu trách nhiệm theo dõi, đôn đốc, kiểm tra, tổng hợp tình hình và báo cáo Công an tỉnh định kỳ **trước ngày 20/11 hằng năm** hoặc báo cáo đột xuất khi có yêu cầu.

2. Các phòng chuyên môn và đơn vị trực thuộc

Trưởng các phòng chuyên môn và đơn vị trực thuộc chịu trách nhiệm trước Giám đốc Ban quản lý về công tác an toàn thông tin, an ninh mạng đối với máy tính, thiết bị, dữ liệu thuộc phạm vi quản lý; đồng thời, tổ chức quán triệt đến toàn thể viên chức, người lao động thuộc phòng, đơn vị thực hiện nghiêm túc Kế hoạch này.

Trên đây là Kế hoạch triển khai thực hiện Quyết định số 515/QĐ-TTg ngày 30 tháng 3 năm 2026 của Thủ tướng Chính phủ phê duyệt Đề án “Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia” của Ban quản lý Vườn Quốc gia Núi Chúa - Phước Bình, đề nghị các phòng, đơn vị trực thuộc khẩn trương, nghiêm túc tổ chức triển khai thực hiện./.

Nơi nhận:

- Ban Giám đốc;
- Các phòng, đơn vị trực thuộc;
- Lưu: VT, HCTC.PTT

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**



Trần Văn Khang



Phụ lục
DANH MỤC NHIỆM VỤ TRIỂN KHAI THỰC HIỆN QUYẾT ĐỊNH SỐ 515/QĐ-TTg
NGÀY 30 THÁNG 3 NĂM 2026 CỦA THỦ TƯỚNG CHÍNH PHỦ
CỦA BAN QUẢN LÝ VQG NÚI CHÚA – PHƯỚC BÌNH

STT	Nhiệm vụ cụ thể	Đơn vị chủ trì	Đơn vị phối hợp	Thời gian triển khai	Thời gian hoàn thành	Sản phẩm, kết quả đầu ra
1	Rà soát, kiện toàn đầu mối, lực lượng chuyên trách, kiêm nhiệm bảo vệ an ninh mạng tại đơn vị.	Phòng HC-TC	Các phòng, đơn vị trực thuộc	Quý II/2026	Hoàn thành trước 30/09/2026; cập nhật thường xuyên	Danh sách đầu mối; quyết định phân công; mô tả nhiệm vụ, yêu cầu năng lực
2	Khảo sát nhu cầu, đánh giá hiện trạng năng lực và xây dựng kế hoạch đào tạo, bồi dưỡng an ninh mạng giai đoạn 2026-2030 theo nhóm đối tượng, vị trí việc làm và cấp độ hệ thống thông tin.	Các phòng, đơn vị trực thuộc		Quý III/2026	Quý IV/2026; cập nhật hằng năm	Đăng ký danh sách theo yêu cầu của cấp trên
3	Đăng ký bồi dưỡng nghiệp vụ quản lý, chỉ đạo, quản trị rủi ro và trách nhiệm người đứng đầu về bảo đảm an ninh mạng cho lãnh đạo, quản lý.	Phòng HC-TC	Các phòng, đơn vị trực thuộc	Từ Quý I/2027	Hằng năm đến 2030	Đăng ký danh sách theo yêu cầu của cấp trên
4	Tham gia đào tạo kiến thức, kỹ năng an ninh mạng, an ninh dữ liệu cho viên chức, người lao động và người dùng cuối; kết hợp trực tiếp, trực tuyến và kiểm tra đánh giá sau khóa học.	Các phòng, đơn vị trực thuộc		Từ Quý I/2027 (năm 2026 đã thực hiện)	Hằng năm đến 2030	Chương trình, học liệu, hệ thống kiểm tra; 100% người dùng được phổ biến, cập nhật kiến thức theo lộ trình.
5	Tham gia diễn tập chuyên đề, diễn tập bàn, diễn tập thực chiến có kiểm soát trong phạm vi quản lý của đơn vị	Các phòng, đơn vị trực thuộc		Từ năm 2026	Ít nhất 01 cuộc/đơn vị/năm	Danh sách tham gia; phương án ứng cứu tại chỗ.
6	Tiếp nhận và chia sẻ thông tin tình báo an ninh mạng, lỗ hổng, mã độc, chỉ dấu tấn công và cảnh báo sớm; kết nối, chia sẻ với nền tảng quốc gia theo hướng dẫn.	Phòng HC-TC	Các phòng, đơn vị trực thuộc	Năm 2027	Năm 2028; vận hành thường xuyên	Nền tảng/kênh chia sẻ thông tin; quy trình phân loại, bảo mật; bản tin cảnh báo định kỳ và đột xuất.

7	Triển khai Bộ chỉ số và thực hiện đánh giá năng lực bảo đảm an ninh mạng đối với đơn vị	Phòng HC-TC	Các phòng, đơn vị trực thuộc	Năm 2027	Thí điểm năm 2027; đánh giá hằng năm	Triển khai Bộ chỉ số theo hướng dẫn của Bộ Công an, phương pháp chấm điểm; báo cáo xếp hạng/đánh giá; kế hoạch khắc phục theo mức độ rủi ro.
8	Tổ chức kiểm tra, đánh giá rủi ro, kiểm thử xâm nhập, rà quét lỗ hổng, kiểm toán an ninh mạng đối với hệ thống thông tin theo kế hoạch và khi có yêu cầu.	Phòng HC-TC	Các phòng, đơn vị trực thuộc	Từ Quý II/2026	Hằng năm đến 2030	Kế hoạch kiểm tra; báo cáo kỹ thuật; danh sách lỗ hổng, điểm yếu; biên bản xác nhận khắc phục và tái kiểm tra.
9	Khảo sát, đánh giá hiện trạng hạ tầng, trang thiết bị, phần mềm, bản quyền và công cụ chuyên dụng của lực lượng bảo vệ an ninh mạng; xây dựng danh mục đầu tư ưu tiên giai đoạn 2026-2030.	Các phòng, đơn vị trực thuộc		Quý II/2026	Quý I/2027; cập nhật hằng năm	Báo cáo hiện trạng và khoảng trống năng lực; danh mục, cấu hình, dự toán sơ bộ; lộ trình đầu tư thống nhất.
10	Tổ chức tuyên truyền nâng cao nhận thức, kỹ năng an ninh mạng; cảnh báo phương thức, thủ đoạn lừa đảo, tấn công mạng.	Các phòng, đơn vị trực thuộc		Từ Quý II/2026	Hằng năm đến 2030	Kế hoạch truyền thông.
11	Tham gia khóa học trực tuyến, học liệu số, bộ công cụ tự kiểm tra và mô hình “Bình dân học vụ số” về an ninh mạng cho viên chức và người lao động	Các phòng, đơn vị trực thuộc		Năm 2026	Hằng năm đến 2030; cập nhật thường xuyên	Khóa học/học liệu số; nền tảng hoặc chuyên mục trực tuyến; bộ câu hỏi, công cụ tự đánh giá; thống kê người học.
12	Xây dựng nội dung, lập dự toán và đề xuất nguồn kinh phí thực hiện các nhiệm vụ được giao; gửi cơ quan có thẩm quyền tổng hợp.	Phòng HC-TC (Bộ phận tài chính)	Các phòng, đơn vị trực thuộc	Hằng năm, từ năm 2026	Theo chu kỳ ngân sách đến 2030	Hồ sơ đề xuất và dự toán kinh phí của từng nhiệm vụ được lập đầy đủ; kinh phí được tổng hợp, xem xét bố trí theo khả năng cân đối ngân sách và quy định hiện hành.
13	Theo dõi, kiểm tra, đôn đốc; thực hiện chế độ báo cáo hằng năm, báo cáo đột xuất; tổ chức sơ kết giữa kỳ và tổng kết Kế hoạch.	Phòng HC-TC	Các phòng, đơn vị trực thuộc	Từ Quý III/2026	Báo cáo hằng năm; sơ kết năm 2028; tổng kết năm 2030	Báo cáo tiến độ, chỉ tiêu, sản phẩm; biên bản kiểm tra; báo cáo sơ kết, tổng kết; đề xuất điều chỉnh và nhiệm vụ giai đoạn tiếp theo.