

KẾ HOẠCH**Triển khai thực hiện Chiến lược An toàn, An ninh mạng quốc gia,
chủ động ứng phó với các thách thức từ không gian mạng
đến năm 2025, tầm nhìn 2030**

(Kèm theo Quyết định số: /QĐ-BVHTTDL ngày / /2023
của Bộ trưởng Bộ Văn hóa, Thể thao và Du lịch)

Thực hiện Quyết định số 964/QĐ-TTg ngày 10/8/2022 của Thủ tướng Chính phủ về “Phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030” (sau đây gọi tắt là *Chiến lược*), Bộ Văn hóa, Thể thao và Du lịch (Bộ VHTTDL) ban hành Kế hoạch triển khai thực hiện như sau:

I. MỤC ĐÍCH, YÊU CẦU**1. Mục đích**

- Tổ chức nghiên cứu, học tập, quán triệt các nội dung của Chiến lược và các quan điểm, chủ trương, chính sách, pháp luật của Đảng, Nhà nước về bảo đảm an toàn, an ninh mạng, ứng phó với thách thức từ không gian mạng.

- Xác định rõ nội dung, trách nhiệm của các đơn vị liên quan trong thực hiện Chiến lược. Tạo chuyển biến mạnh mẽ trong nhận thức, trách nhiệm về bảo đảm an toàn, an ninh mạng, ứng phó với các thách thức từ không gian mạng. Phối hợp chặt chẽ với cơ quan, đơn vị chức năng liên quan trong quá trình thực hiện nhằm hoàn thành tốt các nhiệm vụ được giao trong phạm vi Bộ VHTTDL.

2. Yêu cầu

- Các cơ quan, đơn vị triển khai thực hiện Chiến lược đảm bảo hiệu quả, đạt các mục tiêu đề ra và phù hợp với điều kiện thực tế của cơ quan, đơn vị mình.

- Nâng cao vai trò tham mưu, đề xuất của các cơ quan, đơn vị về thực hiện nhiệm vụ, giải pháp; Về tăng cường hướng dẫn, đôn đốc, kiểm tra, giám sát; Bảo đảm sự phối hợp chặt chẽ, hiệu quả, kịp thời giữa các cơ quan, đơn vị trong quá trình thực hiện Kế hoạch.

II. MỤC TIÊU**1. Mục tiêu tổng quát**

Xây dựng, phát triển không gian mạng văn minh, lành mạnh là động lực tham gia cuộc Cách mạng công nghiệp lần thứ tư. Năng lực về bảo đảm an toàn thông tin mạng và an ninh mạng (gọi tắt là an toàn, an ninh mạng) được nâng cao, chủ động, sẵn sàng ứng phó với các nguy cơ, thách thức từ không gian mạng nhằm bảo vệ vững chắc chủ quyền, lợi ích, quốc phòng, an ninh quốc gia, trật tự an toàn

xã hội; bảo vệ chủ quyền quốc gia trên không gian mạng và công cuộc chuyển đổi số, quyền và lợi ích hợp pháp của tổ chức, cá nhân trên không gian mạng.

2. Mục tiêu cụ thể đến năm 2025

- Xây dựng được hệ thống thể trận an ninh nhân dân trên không gian mạng có khả năng chỉ huy, kết nối, chia sẻ thông tin, tiếp nhận và xử lý sớm các thông tin gây hại đến không gian mạng quốc gia từ các cơ quan, đơn vị thuộc/trực thuộc Bộ VHTTDL.

- Hình thành lực lượng, mạng lưới bảo đảm an toàn, an ninh mạng tại các cơ quan, đơn vị thuộc/trực thuộc Bộ VHTTDL; đảm bảo mỗi cơ quan, đơn vị có một bộ phận được giao nhiệm vụ làm đầu mối, chịu trách nhiệm về công tác bảo đảm an toàn, an ninh mạng.

- Phấn đấu 50% các cán bộ, công chức, viên chức, người lao động tiếp cận hoạt động nâng cao nhận thức, kỹ năng và công cụ bảo đảm an toàn, an ninh mạng.

- Kinh phí bảo đảm an toàn, an ninh mạng đạt tối thiểu 10% kinh phí chi cho khoa học công nghệ, chuyển đổi số, ứng dụng công nghệ thông tin.

3. Mục tiêu cụ thể đến năm 2030

- Xây dựng được thể trận an ninh nhân dân trên không gian mạng với sự tham gia đông đảo, tích cực của tất cả cán bộ, công chức, viên chức, người lao động, các cơ quan, đơn vị thuộc/trực thuộc Bộ VHTTDL.

- Củng cố, tăng cường lực lượng bảo đảm an toàn, an ninh mạng.

- Phấn đấu 90% các cán bộ, công chức, viên chức, người lao động tiếp cận hoạt động nâng cao nhận thức, kỹ năng và công cụ bảo đảm an toàn, an ninh mạng.

III. NHIỆM VỤ, GIẢI PHÁP (Phụ lục kèm theo).

IV. TỔ CHỨC THỰC HIỆN

Các cơ quan, đơn vị triển khai, quán triệt đầy đủ, nghiêm túc Chiến lược và nội dung Kế hoạch này đến cán bộ, công chức, viên chức, người lao động để nắm bắt và triển khai thực hiện.

1. Trung tâm Công nghệ thông tin

- Tham mưu Lãnh đạo Bộ chỉ đạo sơ kết, tổng kết việc thực hiện Kế hoạch này.

- Tham mưu, đề xuất Lãnh đạo Bộ chỉ đạo, điều phối xử lý các vấn đề mới, quan trọng, liên ngành, chưa được quy định hoặc chồng chéo, phức tạp về an toàn, an ninh mạng trong nội dung Kế hoạch này, cần sự phối hợp giữa các đơn vị đầu mối như Văn phòng Bộ, Tổng cục Du lịch, Tổng cục Thể dục thể thao, các đơn vị thuộc/trực thuộc và các cơ quan chức năng có liên quan.

- Chủ trì, phối hợp hướng dẫn, đôn đốc, kiểm tra các cơ quan, đơn vị triển khai thực hiện các nội dung về an ninh mạng theo Kế hoạch này; Báo cáo Lãnh đạo Bộ tình hình thực hiện và đề xuất, kiến nghị nhiệm vụ mới cho phù hợp với tình hình thực tiễn, đối với các nội dung về an toàn, an ninh mạng theo Chiến lược.

2. Vụ Kế hoạch, Tài chính

- Triển khai cơ chế tiền lương đặc thù cho lực lượng chuyên trách về an toàn thông tin mạng và an ninh mạng trong các cơ quan, đơn vị thuộc Bộ.

- Ưu tiên bố trí kinh phí ngân sách để triển khai các nhiệm vụ của Kế hoạch theo quy định của pháp luật về đầu tư công, pháp luật về ngân sách nhà nước.

3. Các đơn vị đầu mối: Văn phòng Bộ, Tổng cục Du lịch, Tổng cục Thể dục thể thao

- Chủ trì, phối hợp với Trung tâm Công nghệ thông tin tổ chức thực hiện các nhiệm vụ được giao theo Kế hoạch.

- Đẩy mạnh hoạt động bảo đảm an toàn, an ninh mạng trong phạm vi quản lý; tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật, hướng dẫn nghiệp vụ Trung tâm CNTT và quy định của pháp luật; ưu tiên sử dụng sản phẩm, giải pháp, dịch vụ an toàn thông tin mạng “Make in Vietnam”, an ninh mạng tự chủ. Gắn kết công tác bảo đảm an toàn, an ninh mạng với công tác triển khai chuyển đổi số, ứng dụng công nghệ thông tin, phát triển Chính quyền điện tử, hướng tới Chính quyền số, phát triển đô thị thông minh, kinh tế số và xã hội số.

- Chủ động rà soát, phát hiện và xử lý hoặc phối hợp với các cơ quan chức năng có thẩm quyền xử lý thông tin vi phạm pháp luật trên môi trường mạng thuộc phạm vi quản lý. Tăng cường hoạt động thanh tra, kiểm tra, công bố và xử lý nghiêm các hành vi vi phạm.

- Ưu tiên bố trí nguồn lực (nhân lực, kinh phí) và điều kiện cần thiết, để triển khai hoạt động bảo đảm an toàn, an ninh mạng trong hoạt động nội bộ của cơ quan, tổ chức và lĩnh vực quản lý.

- Kiểm tra, đánh giá và báo cáo hàng năm hoặc đột xuất theo hướng dẫn của Trung tâm Công nghệ thông tin về tình hình, kết quả triển khai thực hiện Kế hoạch, để tổng hợp, báo cáo theo quy định.

4. Các cơ quan, đơn vị liên quan

Căn cứ nội dung Kế hoạch này, tổ chức triển khai công tác bảo đảm an toàn, an ninh mạng trong hoạt động của cơ quan, đơn vị mình theo hướng dẫn của Trung tâm Công nghệ thông tin.

Trong quá trình triển khai thực hiện Kế hoạch nếu có khó khăn, vướng mắc, các đơn vị chủ động phối hợp với Trung tâm Công nghệ thông tin để tổng hợp báo cáo Lãnh đạo Bộ xem xét, quyết định./.

Phụ lục**NHIỆM VỤ, GIẢI PHÁP THỰC HIỆN CHIẾN LƯỢC AN TOÀN, AN NINH MẠNG QUỐC GIA,
CHỦ ĐỘNG ỨNG PHÓ VỚI CÁC THÁCH THỨC TỪ KHÔNG GIAN MẠNG ĐẾN NĂM 2025, TẦM NHÌN 2030**

(Kèm theo Quyết định số: /QĐ-BVHTTDL ngày / /2023
của Bộ trưởng Bộ Văn hóa, Thể thao và Du lịch)

TT	NHIỆM VỤ	GIẢI PHÁP	ĐƠN VỊ THỰC HIỆN	THỜI GIAN DỰ KIẾN
1.	Tăng cường vai trò lãnh đạo của Đảng, quản lý của Nhà nước	<p>Thống nhất nhận thức từ Bộ tới các cơ quan đơn vị trực thuộc về bảo đảm an toàn, an ninh mạng là trách nhiệm của cả hệ thống chính trị, trong đó Trung tâm Công nghệ thông tin điều phối chung sự phối hợp giữa các đơn vị đầu mối (Văn phòng Bộ, Tổng cục Thể dục thể thao, Tổng cục Du lịch...). Các đơn vị này chủ động, phối hợp thực hiện theo chức năng, nhiệm vụ được giao.</p> <p>Thường xuyên phổ biến, quán triệt chủ trương của Đảng, chính sách, pháp luật của Nhà nước về an toàn, an ninh mạng, coi đây là nhiệm vụ quan trọng của cả hệ thống chính trị.</p> <p>Nâng cao nhận thức, trách nhiệm của chính quyền trong công tác bảo đảm an toàn, an ninh mạng. Thủ trưởng các cơ quan, đơn vị trực tiếp lãnh đạo, chỉ đạo và chịu trách nhiệm về công tác an toàn, an ninh mạng, chủ động rà soát, xác định rõ những vấn đề trọng tâm, trọng điểm để chỉ đạo thực hiện hiệu quả.</p> <p>Phát huy sự tham gia có hiệu quả của cán bộ, công chức, viên chức, người lao động trong công tác bảo đảm an toàn, an ninh mạng và chủ động ứng phó với các nguy cơ, thách thức từ không gian mạng.</p> <ul style="list-style-type: none"> - Triển khai thực hiện và hình thành được mạng lưới ứng cứu sự cố kết hợp chặt chẽ với Thế trận Quốc phòng toàn dân trên không gian mạng. - Đẩy mạnh phổ biến kỹ năng tham gia không gian mạng an toàn. 	<ul style="list-style-type: none"> - Trung tâm Công nghệ thông tin điều phối chung - Văn phòng Bộ, Tổng cục Du lịch, Tổng cục Thể dục thể thao kiểm tra, hướng dẫn các cơ quan, đơn vị trực thuộc 	Thực hiện thường xuyên

TT	NHIỆM VỤ	GIẢI PHÁP	ĐƠN VỊ THỰC HIỆN	THỜI GIAN DỰ KIẾN
2.	Hoàn thiện hành lang pháp lý	Nghiên cứu, tham mưu, đề xuất Bộ xây dựng, hoàn thiện chính sách, pháp luật về bảo vệ an ninh mạng đồng bộ, thống nhất theo định hướng điều chỉnh đầy đủ các lĩnh vực phát sinh hành vi sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự an toàn xã hội; nâng cao năng lực bảo vệ chủ quyền quốc gia trên không gian mạng theo chức năng, nhiệm vụ được giao.	Trung tâm Công nghệ thông tin chủ trì, phối hợp với các đơn vị có liên quan thực hiện	Thực hiện thường xuyên và khi có yêu cầu của Bộ Công an.
		Nghiên cứu, rà soát, đề xuất sửa đổi, bổ sung văn bản quy phạm pháp luật về an ninh mạng để đồng bộ, thống nhất, toàn diện, đáp ứng được yêu cầu đấu tranh, xử lý vi phạm pháp luật về an ninh mạng.		
		Đề xuất Bộ Thông tin và Truyền thông xây dựng, hoàn thiện chính sách, pháp luật về an toàn thông tin mạng, nhất là các chế tài xử lý vi phạm pháp luật về an toàn thông tin mạng.	Trung tâm Công nghệ thông tin chủ trì	Thực hiện thường xuyên và khi có yêu cầu của Bộ Thông tin và Truyền thông
		Nghiên cứu, rà soát, đề xuất Bộ Thông tin và Truyền thông xây dựng, sửa đổi, bổ sung văn bản quy phạm pháp luật và văn bản hướng dẫn thi hành về bảo đảm an toàn thông tin mạng cho giao dịch điện tử, chuyển đổi số, hạ tầng số, nền tảng số, dữ liệu số, bảo vệ thông tin cá nhân trên mạng.		
		Các cơ quan, đơn vị liên quan theo chức năng, nhiệm vụ được giao tham gia xây dựng cơ chế, chính sách, pháp luật về an toàn, an ninh mạng và đội ngũ vận hành hệ thống thông tin quan trọng của Bộ VHTTDL.	Trung tâm Công nghệ thông tin, các cơ quan liên quan	Thực hiện thường xuyên
3.	Bảo vệ chủ quyền quốc gia trên không gian mạng	Xây dựng năng lực tự chủ, phản ứng trước các hoạt động xâm phạm chủ quyền quốc gia trên không gian mạng.	Trung tâm Công nghệ thông tin, các đơn vị đầu mối, các cơ quan liên quan	Thực hiện thường xuyên
		Trung tâm Công nghệ thông tin các đơn vị đầu mối, các cơ quan liên quan phối hợp bảo vệ chủ quyền quốc gia trên không gian mạng theo đúng chức năng, nhiệm vụ được giao.		
4.	Bảo vệ hạ tầng số, nền tảng số, dữ liệu số, cơ	4.1. Bảo vệ cơ sở hạ tầng không gian mạng trong phạm vi quản lý		

TT	NHIỆM VỤ	GIẢI PHÁP	ĐƠN VỊ THỰC HIỆN	THỜI GIAN DỰ KIẾN
	sở hạ tầng không gian mạng	Bảo đảm an toàn, an ninh mạng trong quá trình lựa chọn, triển khai các dịch vụ, công nghệ cho cơ sở hạ tầng không gian mạng; ưu tiên sử dụng sản phẩm an toàn, an ninh mạng Việt Nam.	Trung tâm Công nghệ thông tin, các đơn vị đầu mối, các cơ quan liên quan	Thực hiện thường xuyên và theo chỉ đạo của Chính phủ
		Bảo đảm an toàn, an ninh mạng trong quá trình thiết kế, xây dựng, vận hành, khai thác cơ sở hạ tầng không gian mạng. Giám sát, cảnh báo sớm các hành vi vi phạm pháp luật trên không gian mạng trong phạm vi quản lý.		
		Nâng cao năng lực tự chủ về an toàn, an ninh mạng.		
		Bảo đảm an toàn, an ninh mạng cho quá trình triển khai Chính quyền điện tử, chuyển đổi số.		
		4.2. Bảo vệ hạ tầng số		
		Tham mưu Bộ triển khai tiêu chuẩn, quy chuẩn kỹ thuật và tiêu chí kỹ thuật về an toàn thông tin mạng đối với hạ tầng, dịch vụ điện toán đám mây, thiết bị 5G và thiết bị internet kết nối vạn vật (IoT) khi Bộ Thông tin và Truyền thông ban hành, hướng dẫn.	Trung tâm Công nghệ thông tin chủ trì, phối hợp với các cơ quan, đơn vị có liên quan.	Thực hiện thường xuyên
		Theo chức năng, nhiệm vụ được giao, thực hiện thu thập, tổng hợp, phân tích dữ liệu lưu lượng truy cập internet trên môi trường mạng có liên quan nhằm phát hiện các dấu hiệu, nguy cơ để dự báo sớm, kịp thời ngăn chặn hành vi tấn công mạng.		
		Tham mưu, đề xuất tổ chức các Chiến dịch rà quét, xử lý bóc gỡ mã độc thuộc phạm vi Bộ VHTTDL.		
		Phòng chống chiến tranh thông tin, chiến tranh không gian mạng theo chức năng, nhiệm vụ được giao.		
		Phối hợp với các cơ quan liên quan trong công tác chỉ đạo, kiểm tra, đánh giá các nhà cung cấp dịch vụ nền tảng số thực thi trách nhiệm và sứ mệnh bảo đảm an toàn, an ninh mạng.		
Trung tâm Công nghệ thông tin, các đơn vị đầu mối, các cơ quan liên quan	Thực hiện thường xuyên			

TT	NHIỆM VỤ	GIẢI PHÁP	ĐƠN VỊ THỰC HIỆN	THỜI GIAN DỰ KIẾN
		<p>Phối hợp kiểm tra, đánh giá, bảo đảm an ninh mạng theo chức năng, nhiệm vụ được giao.</p>		
		<p>Lựa chọn sử dụng dịch vụ viễn thông, internet và dịch vụ hạ tầng số được công khai mức độ an toàn, an ninh mạng. Ưu tiên sử dụng sản phẩm an toàn, an ninh mạng Make in Vietnam.</p>	<p>Trung tâm Công nghệ thông tin, các đơn vị đầu mối, các cơ quan liên quan</p>	<p>Thực hiện thường xuyên</p>
		<p>Chủ động thông báo cho lực lượng chức năng khi xảy ra các hành vi vi phạm pháp luật trên không gian mạng; thực hiện hoặc thông báo, phối hợp với doanh nghiệp hạ tầng số khắc phục, xử lý hoặc từng bước thay thế thiết bị đầu cuối có dấu hiệu mất an toàn thông tin mạng.</p>		
		4.3. Bảo vệ nền tảng số		
		<p>Xác định cấp độ an toàn thông tin và triển khai phương án bảo đảm an toàn hệ thống thông tin theo cấp độ đối với nền tảng số.</p>	<p>Trung tâm Công nghệ thông tin, các đơn vị đầu mối, các cơ quan liên quan</p>	<p>Thực hiện thường xuyên</p>
		<p>Phát triển nền tảng số có khả năng tự bảo vệ; có các công cụ sàng lọc, phát hiện, xử lý, gỡ bỏ thông tin vi phạm pháp luật trên nền tảng số.</p>		
		<p>Công khai chính sách quản lý, sử dụng thông tin, dữ liệu của người sử dụng trên nền tảng số. Bảo đảm an toàn thông tin cá nhân, thông tin về tài khoản, mật khẩu tin nhắn, lịch sử giao dịch của người sử dụng dịch vụ nền tảng số.</p>		
		<p>Chủ động phát hiện, ngăn chặn, xử lý, xóa bỏ tin giả, thông tin vi phạm pháp luật hoặc cung cấp các bằng chứng, để truy vết, xác định nguồn gốc thông tin; xử lý, xóa bỏ thông tin vi phạm pháp luật theo yêu cầu của cơ quan chức năng có thẩm quyền.</p>		
		<p>Phòng, chống chiến tranh thông tin, chiến tranh không gian mạng theo chức năng, nhiệm vụ được giao.</p>		

TT	NHIỆM VỤ	GIẢI PHÁP	ĐƠN VỊ THỰC HIỆN	THỜI GIAN DỰ KIẾN
		<p>Phối hợp với các cơ quan liên quan trong công tác chỉ đạo, kiểm tra, đánh giá các doanh nghiệp cung cấp dịch vụ nền tảng số thực thi trách nhiệm và sứ mệnh bảo đảm an toàn, an ninh mạng.</p>	<p>đầu mối, các cơ quan liên quan</p>	
		<p>Lựa chọn sử dụng dịch vụ nền tảng số an toàn, lành mạnh.</p>	<p>Tất cả các cơ quan, đơn vị, cá nhân sử dụng dịch vụ</p>	<p>Thực hiện thường xuyên</p>
		<p>Thận trọng khi cung cấp thông tin, dữ liệu cá nhân trên nền tảng số; bảo mật tài khoản, mật khẩu để không bị lộ lọt, lợi dụng thực hiện hành vi vi phạm pháp luật.</p>		
		<p>Tuân thủ các quy tắc ứng xử, không đăng tải, lan truyền các nội dung vi phạm pháp luật trên môi trường mạng.</p>		
		<p>Chia sẻ, lan tỏa các thông tin tích cực; cảnh báo và phản ánh, tố giác các hành vi vi phạm pháp luật.</p>		
		<p>4.4. Bảo vệ dữ liệu của các tổ chức, cá nhân</p>		
		<p>Tham mưu, đề xuất xây dựng chính sách, pháp luật về bảo vệ dữ liệu, nhằm bảo vệ quyền và lợi ích hợp pháp của tổ chức, cá nhân, đặc biệt là dữ liệu quan trọng quốc gia.</p>	<p>Trung tâm Công nghệ thông tin, các đơn vị đầu mối, các cơ quan liên quan</p>	<p>Thực hiện thường xuyên</p>
		<p>Bảo đảm an ninh mạng, an toàn thông tin mạng theo cấp độ cho các cơ sở dữ liệu quốc gia và cơ sở dữ liệu quan trọng của ngành văn hóa, thể thao, du lịch và gia đình.</p>		
		<p>Thiết lập cơ chế đánh giá rủi ro bảo mật dữ liệu tập trung, hiệu quả và có thẩm quyền; báo cáo, chia sẻ thông tin, giám sát và cảnh báo sớm; tăng cường thu thập, phân tích, nghiên cứu, phán đoán và cảnh báo sớm về thông tin rủi ro bảo mật dữ liệu. Xây dựng cơ chế phản ứng khẩn cấp trong trường hợp xảy ra sự cố bảo mật dữ liệu.</p>		
<p>5.</p>	<p>Bảo vệ hệ thống thông tin của các cơ quan Đảng, Nhà nước</p>	<p>Nâng cao trách nhiệm tự bảo vệ hệ thống thông tin thuộc phạm vi quản lý. Gắn trách nhiệm của người đứng đầu cơ quan chủ quản hệ thống thông tin với trách nhiệm bảo đảm an toàn, an ninh mạng.</p>	<p>Chủ quản hệ thống thông tin phối hợp với Trung tâm Công</p>	<p>Thực hiện thường xuyên</p>

TT	NHIỆM VỤ	GIẢI PHÁP	ĐƠN VỊ THỰC HIỆN	THỜI GIAN DỰ KIẾN
		<p>Xây dựng, cập nhật, vận hành hệ thống thông tin theo tiêu chuẩn, quy chuẩn kỹ thuật về an toàn, an ninh mạng.</p> <p>Rà soát, lập hồ sơ đề nghị đưa các hệ thống thông tin trọng yếu, phù hợp với quy định của pháp luật vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.</p> <p>Thực hiện nghiêm túc các quy định pháp luật về bảo vệ an ninh mạng; xác định cấp độ và trách nhiệm bảo đảm an toàn hệ thống thông tin theo từng cấp độ và triển khai mô hình bảo vệ 4 lớp trước khi đưa vào sử dụng.</p> <p>Chủ động giám sát, kịp thời phát hiện nguy cơ mất an toàn, an ninh mạng trong quá trình thi công, lắp đặt thiết bị trong các hệ thống thông tin. Ưu tiên sử dụng sản phẩm, giải pháp an toàn, an ninh mạng Make in Vietnam.</p> <p>Đầu tư nguồn lực, thường xuyên nâng cấp hệ thống, cập nhật bản quyền, nâng cao nhận thức và kỹ năng an toàn, an ninh mạng cho cán bộ, công chức, viên chức và người lao động, ít nhất 1 năm/1 lần tổ chức hoặc tham gia diễn tập, hướng dẫn, kiểm tra, ứng phó và ứng cứu sự cố an toàn, an ninh mạng.</p> <p>Phối hợp với đơn vị chuyên trách để báo cáo, đề xuất kết nối với Trung tâm An ninh mạng quốc gia để giám sát an ninh mạng.</p>	nghệ thông tin và các đơn vị liên quan	
		<p>Chủ động xây dựng kế hoạch, tổ chức kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia và các hệ thống thông tin quan trọng dùng chung của Bộ.</p> <p>Tham mưu, đề xuất Bộ tổ chức diễn tập thực chiến về an ninh mạng cấp Bộ, có sự tham gia của các chủ quản hệ thống thông tin quan trọng về an ninh quốc gia, hệ thống thông tin quan trọng dùng chung của Bộ, tổ chức, doanh nghiệp bảo đảm an ninh mạng.</p>	Trung tâm Công nghệ thông tin chủ trì, phối hợp với các đơn vị có liên quan.	Thực hiện thường xuyên và theo Kế hoạch

TT	NHIỆM VỤ	GIẢI PHÁP	ĐƠN VỊ THỰC HIỆN	THỜI GIAN DỰ KIẾN
		<p>Xây dựng, hình thành mạng lưới ứng phó, khắc phục sự cố an ninh mạng, lấy lực lượng chuyên trách bảo vệ an ninh mạng làm trung tâm, phối hợp chặt chẽ với các cơ quan, tổ chức, cá nhân trong ứng phó, khắc phục sự cố an ninh mạng.</p> <p>Chủ trì, phối hợp các đơn vị đầu mối, các đơn vị có liên quan xây dựng cơ chế phối hợp, chia sẻ thông tin giám sát an toàn, an ninh mạng hệ thống thông tin của các đơn vị thuộc Bộ VHTTDL.</p> <p>Phối hợp với chủ quản hệ thống thông tin khắc phục, xử lý nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật, phần cứng độc hại.</p> <p>Triển khai các biện pháp phòng ngừa, đấu tranh, xử lý hành vi xâm phạm an ninh mạng, hoạt động của các đối tượng, thế lực thù địch sử dụng không gian mạng xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự an toàn xã hội.</p>		
		<p>Thực hiện chuyển đổi IPv6 cho Bộ VHTTDL theo “Kế hoạch chuyển đổi IPv6 cho các hệ thống công nghệ thông tin thuộc Bộ Văn hóa, Thể thao và Du lịch giai đoạn 2021-2025” được Lãnh đạo Bộ VHTTDL phê duyệt ngày 22/11/2021 nhằm giải quyết vấn đề cạn kiệt địa chỉ IP trong IPv4; Cải thiện bảo mật và Tăng tốc độ và hiệu suất mạng.</p> <p>Triển khai Nền tảng điện toán đám mây riêng của Bộ đáp ứng yêu cầu bảo đảm an toàn thông tin mạng, tạo cơ sở hạ tầng an toàn cho các ứng dụng Chính quyền điện tử dùng chung.</p> <p>Triển khai, phát triển Nền tảng Điều hành, chỉ huy an toàn thông tin mạng tập trung, kết nối, phân tích dữ liệu lớn, chia sẻ thông tin rủi ro an toàn thông tin mạng với 100% SOC của các cơ quan, đơn vị thuộc Bộ, nhằm dự báo, cảnh báo sớm, giúp ngăn chặn, xử lý kịp thời sự cố an toàn thông tin mạng, tránh thiệt hại trên diện rộng.</p>	Trung tâm Công nghệ thông tin chủ trì.	Thực hiện thường xuyên và theo hướng dẫn của Bộ Thông tin và Truyền thông

TT	NHIỆM VỤ	GIẢI PHÁP	ĐƠN VỊ THỰC HIỆN	THỜI GIAN DỰ KIẾN
		<p>Triển khai, phát triển Nền tảng rà quét lỗ hổng bảo mật nhằm phòng ngừa sự cố mất an toàn thông tin mạng cho các ứng dụng Chính quyền điện tử của cơ quan, đơn vị thuộc Bộ.</p> <p>Đánh giá và gán nhãn tín nhiệm mạng đối với các website.</p> <p>Phát triển Mạng lưới ứng cứu sự cố an toàn thông tin mạng thuộc phạm vi quản lý, nhằm điều phối kịp thời, phối hợp đồng bộ, hiệu quả các lực lượng, để bảo đảm an toàn thông tin mạng.</p> <p>Thực hiện giám sát, cảnh báo sớm để bảo vệ hệ thống thông tin của các đơn vị thuộc Bộ VHTTDL.</p>		
6.	Bảo vệ hệ thống thông tin của các lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin	<p>Triển khai phương án bảo đảm an toàn thông tin theo cấp độ và mô hình bảo vệ 4 lớp đối với hệ thống thông tin của các lĩnh vực quan trọng.</p> <p>Đầu tư nâng cao nhận thức cho các tổ chức, cá nhân liên quan về bảo đảm an toàn thông tin mạng cho các hệ thống thông tin của các lĩnh vực quan trọng.</p> <p>Ít nhất 1 năm/1 lần tổ chức diễn tập, hướng dẫn, kiểm tra, ứng phó và ứng cứu sự cố an toàn thông tin cho các lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin và hệ thống thông tin quan trọng.</p>	Chủ quản hệ thống thông tin	Thực hiện thường xuyên
		<p>Chia sẻ thông tin về nguy cơ, rủi ro an toàn thông tin mạng cho chủ quản hệ thống thông tin.</p> <p>Hướng dẫn, kiểm tra, đôn đốc công tác bảo đảm an toàn thông tin mạng đối với các hệ thống thông tin quan trọng thuộc phạm vi quản lý.</p>	Trung tâm Công nghệ thông tin chủ trì, phối hợp với các đơn vị có liên quan.	Thực hiện thường xuyên
7.	Tạo lập niềm tin số, xây dựng môi trường mạng trung thực, văn minh,	<p>Xây dựng cơ chế, thiết lập đường dây nóng, hệ thống tiếp nhận, xử lý thông tin về tội phạm mạng từ không gian mạng, phản ánh kịp thời, trực tiếp thông tin, hành vi vi phạm pháp luật trên không gian mạng.</p>	Trung tâm Công nghệ thông tin	Thực hiện thường xuyên

TT	NHIỆM VỤ	GIẢI PHÁP	ĐƠN VỊ THỰC HIỆN	THỜI GIAN DỰ KIẾN
	lành mạnh và phòng, chống vi phạm pháp luật trên không gian mạng	Xây dựng cơ chế phối hợp liên ngành với các cơ quan, đơn vị, lực lượng, các tổ chức, doanh nghiệp chuyên trách bảo vệ an ninh mạng theo quy định của pháp luật trong thực hiện công tác phòng ngừa, phát hiện, điều tra, xử lý các vi phạm pháp luật trên không gian mạng và chống khủng bố mạng.		
		Hướng dẫn tổ chức, cá nhân thay đổi thói quen, hành vi trên môi trường mạng theo các chuẩn mực an toàn.	Trung tâm Công nghệ thông tin chủ trì, phối hợp với các đơn vị có liên quan.	Thực hiện thường xuyên và theo chỉ đạo của Chính phủ
		Đổi mới phương thức tuyên truyền, nâng cao nhận thức, phổ biến kiến thức và thay đổi thái độ của các cán bộ, công chức, viên chức về an toàn thông tin với quan điểm lấy cộng đồng làm trung tâm qua các hình thức như: ứng dụng trên điện thoại, mạng xã hội...		
		Phát hiện, xử lý các hành vi đăng tải, lưu trữ, trao đổi trái phép thông tin, tài liệu có nội dung bí mật nhà nước trong phạm vi quản lý.	Trung tâm Công nghệ thông tin, các đơn vị đầu mối	Thực hiện thường xuyên
		Phối hợp với các cơ quan, đơn vị thuộc Bộ thực hiện phòng ngừa, phát hiện, xử lý hành vi tấn công mạng, hành vi chống phá Đảng, Nhà nước; Phòng, chống khủng bố mạng đối với các hệ thống thông tin trong phạm vi quản lý.		
		Giám sát, phát hiện và phối hợp với cơ quan chức năng và các doanh nghiệp nền tảng số xử lý tin giả, thông tin vi phạm pháp luật trong phạm vi quản lý.	Các đơn vị có liên quan	Thực hiện thường xuyên
		Phát triển các website, trang mạng xã hội, tài khoản trên môi trường mạng uy tín, nhiều tương tác để tuyên truyền, định hướng thông tin, dư luận và phản bác hiệu quả các thông tin tiêu cực về đất nước, con người Việt Nam, hình ảnh địa phương.		

TT	NHIỆM VỤ	GIẢI PHÁP	ĐƠN VỊ THỰC HIỆN	THỜI GIAN DỰ KIẾN
8.	Làm chủ, tự chủ công nghệ, sản phẩm, dịch vụ đủ khả năng chủ động ứng phó với các thách thức từ không gian mạng	Báo cáo, đề xuất Bộ trong xây dựng chiến lược từng bước tiếp thu, kế thừa công nghệ, sản phẩm, dịch vụ an ninh mạng, chuyển giao công nghệ. Khuyến khích và tôn vinh tinh thần đổi mới sáng tạo về công nghệ, sản phẩm, dịch vụ an ninh mạng.	Trung tâm Công nghệ thông tin	Thực hiện thường xuyên
		Thúc đẩy triển khai mô hình an toàn thông tin mạng như dịch vụ (Security as a Service).	Trung tâm Công nghệ thông tin	Thực hiện theo kế hoạch
9.	Đào tạo và phát triển nguồn nhân lực	Nghiên cứu, đề xuất, triển khai phương án thúc đẩy hoạt động đào tạo và phát triển nguồn nhân lực an toàn thông tin giai đoạn 2021 - 2025; Báo cáo, đề xuất Bộ xây dựng cơ chế, chính sách, pháp luật về đào tạo nguồn nhân lực về bảo đảm an ninh mạng. Phát triển đội ngũ chuyên gia về an toàn thông tin mạng.	Trung tâm Công nghệ thông tin chủ trì, phối hợp với các đơn vị có liên quan.	Thực hiện thường xuyên và theo chỉ đạo của Chính phủ, Bộ Thông tin và Truyền thông
		Hướng dẫn, thúc đẩy triển khai quy định chuẩn kỹ năng an toàn thông tin mạng.		
		Đề xuất Bộ tuyên dương, khen thưởng kịp thời đối với các cơ quan, tổ chức, doanh nghiệp, cá nhân có cống hiến cho an toàn thông tin mạng.		
		Xây dựng đội ngũ kỹ sư an ninh mạng chất lượng cao, đóng vai trò quan trọng trong việc quản lý, vận hành, tiếp thu, chuyển giao tri thức về an ninh mạng.		
10.	Tuyên truyền, phổ biến, nâng cao nhận thức và kỹ năng an toàn, an ninh mạng	Tăng cường các hoạt động tuyên truyền, nâng cao nhận thức và phổ biến kiến thức, trang bị kỹ năng bảo đảm an toàn thông tin tới toàn thể cán bộ, công chức, viên chức thuộc Bộ VHTTDL.	Trung tâm Công nghệ thông tin chủ trì, phối hợp với các đơn vị có liên quan.	Thực hiện thường xuyên và theo chỉ đạo của Chính phủ, Bộ Thông tin và Truyền thông
		Triển khai các khóa học trực tuyến tuyên truyền, phổ biến kỹ năng an toàn thông tin cơ bản cho người dùng.		

TT	NHIỆM VỤ	GIẢI PHÁP	ĐƠN VỊ THỰC HIỆN	THỜI GIAN DỰ KIẾN
		<p>Thiết lập các kênh, mạng xã hội để tuyên truyền, nâng cao nhận thức về bảo đảm an ninh mạng đối với quần chúng nhân dân về âm mưu, phương thức, thủ đoạn, các hành vi xâm phạm an ninh mạng, nâng cao sức đề kháng trước các thông tin xấu độc, thủ đoạn của các loại tội phạm sử dụng công nghệ cao.</p> <p>Cung cấp kịp thời các thông tin chính thống, để cán bộ, công chức, viên chức, người lao động nắm bắt, cùng phản biện tin giả, thông tin vi phạm pháp luật trên môi trường mạng.</p> <p>Trong phạm vi quản lý, tổ chức triển khai các kế hoạch tuyên truyền, phổ biến về thói quen, trách nhiệm, kỹ năng an toàn, an ninh mạng cho cán bộ, công chức, viên chức, người lao động khi tham gia hoạt động trên không gian mạng.</p> <p>Các đơn vị có chức năng truyền thông, báo chí tăng cường thông tin về xu hướng, kiến thức, tình hình, nguy cơ, hậu quả an toàn, an ninh mạng thế giới và Việt Nam.</p> <p>Triển khai thực hiện cơ chế tiền lương đặc thù cho lực lượng chuyên trách về an toàn thông tin mạng và an ninh mạng trong các cơ quan, tổ chức nhà nước.</p>	<p>Trung tâm Công nghệ thông tin, các cơ quan, đơn vị có liên quan</p>	<p>Thực hiện thường xuyên</p>
11.	Đầu tư nguồn lực và bảo đảm kinh phí thực hiện	<p>Ưu tiên bố trí nguồn lực, để triển khai các Đề án và xây dựng các hệ thống kỹ thuật bảo đảm an toàn, an ninh mạng.</p> <p>Bố trí kinh phí chi cho an toàn, an ninh mạng đạt tối thiểu 10% kinh phí chi cho khoa học công nghệ, chuyển đổi số, ứng dụng công nghệ thông tin.</p> <p>Bảo đảm kinh phí thực hiện các nhiệm vụ thuộc Chiến lược do Bộ VHTTDL thực hiện.</p>	<p>Vụ Kế hoạch Tài chính chủ trì, hướng dẫn các cơ quan, đơn vị</p>	<p>Thực hiện thường xuyên</p>

TT	NHIỆM VỤ	GIẢI PHÁP	ĐƠN VỊ THỰC HIỆN	THỜI GIAN DỰ KIẾN
		<p>Ưu tiên nguồn vốn khoa học và công nghệ, nguồn vốn từ các chương trình quốc gia để phát triển công nghệ cao, chương trình phát triển sản phẩm quốc gia để phát triển sản phẩm, dịch vụ, giải pháp nội địa và các nhiệm vụ nghiên cứu, phát triển, chuyển giao công nghệ thuộc Chiến lược.</p>		