CHÍNH PHỦ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 329/2026/NĐ-CP	*Hà Nội, ngày 19 tháng 8 năm 2026*

NGHỊ ĐỊNH
Quy định về lực lượng bảo vệ an ninh mạng

Căn cứ Luật Tổ chức Chính phủ số 63/2025/QH15;

Căn cứ Luật An ninh mạng số 116/2025/QH15;

Theo đề nghị của Bộ trưởng Bộ Công an;

Chính phủ ban hành Nghị định quy định về lực lượng bảo vệ an ninh mạng.

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Nghị định này quy định về lực lượng bảo vệ an ninh mạng bao gồm tổ chức, hoạt động, phối hợp, huy động tham gia bảo vệ an ninh mạng; chính sách đãi ngộ, thu hút nhân tài và trách nhiệm tổ chức thực hiện.

Điều 2. Đối tượng áp dụng

1. Lực lượng bảo vệ an ninh mạng.

2. Đối tượng áp dụng chính sách đãi ngộ là người thuộc biên chế của lực lượng chuyên trách bảo vệ an ninh mạng.

3. Đối tượng áp dụng chính sách thu hút nhân tài là công dân Việt Nam có trình độ chuyên môn cao, năng lực nổi trội, thành tích xuất sắc hoặc kinh nghiệm thực tiễn nổi bật trong lĩnh vực liên quan trực tiếp đến bảo vệ an ninh mạng; được xem xét tuyển dụng, tiếp nhận, bố trí, sử dụng hoặc ký hợp đồng để tham gia thực hiện nhiệm vụ trong lực lượng chuyên trách bảo vệ an ninh mạng.

4. Cơ quan, tổ chức, cá nhân khác có liên quan đến việc thi hành Nghị định này.

Điều 3. Nguyên tắc tổ chức và hoạt động của lực lượng bảo vệ an ninh mạng

1. Tổ chức, hoạt động của lực lượng bảo vệ an ninh mạng tuân thủ Hiến pháp và pháp luật, bảo đảm chỉ huy thống nhất, phối hợp chặt chẽ, phân định rõ trách nhiệm, thẩm quyền, không chồng chéo, trùng lặp, góp phần bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội, bảo vệ quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

2. Việc huy động, phối hợp lực lượng, áp dụng chính sách đãi ngộ, thu hút nhân tài phải căn cứ vào yêu cầu, tính chất nhiệm vụ, mức độ rủi ro, yêu cầu bảo mật, kết quả thực hiện nhiệm vụ và khả năng cân đối nguồn lực.

3. Cơ quan, tổ chức, cá nhân tham gia bảo vệ an ninh mạng khi thực hiện đúng thẩm quyền, đúng phạm vi nhiệm vụ được bảo vệ quyền, lợi ích và được bảo đảm các điều kiện thực hiện nhiệm vụ theo quy định của pháp luật.

4. Nhà nước khuyến khích nghiên cứu, đổi mới sáng tạo, thử nghiệm có kiểm soát, huy động cộng đồng và hợp tác công - tư trong lĩnh vực an ninh mạng theo quy định của pháp luật.

5. Bộ Quốc phòng quản lý về an ninh mạng đối với nhiệm vụ quân sự, quốc phòng; Bộ Công an quản lý về an ninh mạng đối với các đơn vị Quân đội có hoạt động dân sự, kinh tế theo thẩm quyền; đối với các nội dung giao thoa (nếu có), Bộ Công an và Bộ Quốc phòng thống nhất quy chế phối hợp.

Điều 4. Giải thích từ ngữ

Trong Nghị định này, các từ ngữ dưới đây được hiểu như sau:

1. Lực lượng bảo vệ an ninh mạng bao gồm lực lượng chuyên trách, lực lượng thường trực và lực lượng dự bị tham gia bảo vệ an ninh mạng theo quy định của pháp luật.

2. Mạng lưới, liên minh tham gia bảo vệ an ninh mạng là tập hợp tổ chức, cá nhân có trình độ, năng lực, kinh nghiệm chuyên môn trong lĩnh vực an ninh mạng tự nguyện hợp tác nghiên cứu, đào tạo, tư vấn, ứng cứu sự cố, xử lý lỗ hổng và thực hiện nhiệm vụ khác bảo vệ an ninh mạng theo quy định của pháp luật.

3. Hợp tác tự nguyện tham gia bảo vệ an ninh mạng là việc cơ quan, tổ chức, doanh nghiệp, cá nhân chủ động tham gia mạng lưới, liên minh, chương trình, hoạt động hỗ trợ bảo vệ an ninh mạng trên cơ sở tự nguyện, bình đẳng,

tuân thủ pháp luật và không làm phát sinh thẩm quyền công vụ, trừ trường hợp được cơ quan có thẩm quyền giao nhiệm vụ hoặc huy động theo quy định của pháp luật.

Chương II
LỰC LƯỢNG BẢO VỆ AN NINH MẠNG

Điều 5. Lực lượng chuyên trách bảo vệ an ninh mạng

1. Lực lượng chuyên trách bảo vệ an ninh mạng là lực lượng nòng cốt, được bố trí tại Bộ Công an, Bộ Quốc phòng theo quy định của Luật An ninh mạng và pháp luật có liên quan.

2. Lực lượng chuyên trách bảo vệ an ninh mạng có nhiệm vụ:

a) Tham mưu chính sách, pháp luật về an ninh mạng, an ninh dữ liệu, bảo vệ dữ liệu cá nhân, dự án công nghệ chiến lược theo quy định của pháp luật;

b) Quản lý nhà nước về an ninh mạng, an ninh dữ liệu, bảo vệ dữ liệu cá nhân theo quy định của pháp luật;

c) Thực hiện biện pháp bảo vệ an ninh mạng, an ninh dữ liệu, bảo vệ dữ liệu cá nhân theo quy định của pháp luật;

d) Phòng ngừa, phát hiện, ngăn chặn, xử lý hoạt động xâm phạm an ninh mạng, an ninh dữ liệu, dữ liệu cá nhân theo thẩm quyền;

đ) Điều phối, kiểm tra, hướng dẫn, huấn luyện, diễn tập, ứng cứu sự cố an ninh mạng, an ninh dữ liệu, bảo vệ dữ liệu cá nhân theo quy định của pháp luật;

e) Hợp tác quốc tế về an ninh mạng, an ninh dữ liệu, bảo vệ dữ liệu cá nhân theo quy định của pháp luật;

g) Nhiệm vụ khác theo quy định của pháp luật.

3. Lực lượng chuyên trách bảo vệ an ninh mạng được ưu tiên bảo đảm biên chế, vị trí việc làm, điều kiện làm việc, trang thiết bị chuyên dùng, đào tạo chuyên sâu và được áp dụng chính sách quy định tại Chương III của Nghị định này.

Điều 6. Lực lượng thường trực bảo vệ an ninh mạng

1. Lực lượng thường trực bảo vệ an ninh mạng gồm lực lượng bảo vệ an ninh mạng được bố trí tại bộ, ngành, Ủy ban nhân dân cấp tỉnh, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia và bộ phận thực hiện nhiệm vụ thường trực bảo vệ an ninh mạng đối với hệ thống thông tin, cơ sở dữ liệu của cơ quan, tổ chức, doanh nghiệp.

2. Việc bố trí lực lượng thường trực bảo vệ an ninh mạng tại bộ, ngành, Ủy ban nhân dân cấp tỉnh và cơ quan, tổ chức, doanh nghiệp căn cứ vào quy mô, tính chất, mức độ quan trọng của hệ thống thông tin, quy mô dữ liệu, phạm vi phục vụ, yêu cầu giám sát thường xuyên, liên tục, rủi ro an ninh mạng, an ninh dữ liệu và mức độ phụ thuộc vào dịch vụ, hạ tầng kỹ thuật, chuỗi cung ứng số bên ngoài, theo một hoặc kết hợp một số hình thức sau đây:

a) Bố trí đơn vị hoặc bộ phận chuyên trách thực hiện nhiệm vụ thường trực bảo vệ an ninh mạng;

b) Bố trí nhân sự chuyên trách thực hiện nhiệm vụ thường trực bảo vệ an ninh mạng;

c) Thuê tổ chức, doanh nghiệp cung cấp dịch vụ an ninh mạng theo quy định của pháp luật để hỗ trợ thực hiện nhiệm vụ bảo vệ an ninh mạng cho hệ thống thông tin của cơ quan chủ quản.

3. Cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia bố trí bộ phận hoặc nhân sự chuyên trách bảo vệ an ninh mạng.

4. Lực lượng thường trực bảo vệ an ninh mạng có nhiệm vụ:

a) Bảo vệ an ninh mạng đối với hệ thống thông tin, cơ sở dữ liệu thuộc phạm vi quản lý;

b) Tổ chức quản lý rủi ro, giám sát an ninh mạng, kiểm soát truy cập, phân quyền đối với hệ thống thông tin, cơ sở dữ liệu thuộc phạm vi quản lý;

c) Tham mưu chủ quản hệ thống thông tin báo cáo về sự cố an ninh mạng; thực hiện quy trình ứng cứu sự cố; báo cáo, phối hợp theo cơ chế điều phối quy định của pháp luật; thực hiện chế độ báo cáo định kỳ hoặc đột xuất theo yêu cầu của cơ quan có thẩm quyền theo quy định của pháp luật;

d) Tổ chức hoặc tham mưu cơ quan chủ quản hệ thống thông tin tổ chức kiểm tra, đánh giá việc tuân thủ quy định về bảo vệ an ninh mạng, an ninh dữ liệu, bảo vệ dữ liệu cá nhân đối với hệ thống thông tin, cơ sở dữ liệu thuộc phạm vi quản lý;

đ) Tổ chức hoặc tham mưu cơ quan chủ quản hệ thống thông tin tổ chức đào tạo, bồi dưỡng, huấn luyện, diễn tập bảo vệ an ninh mạng;

e) Tham gia bảo vệ an ninh mạng theo quy định của pháp luật;

g) Trao đổi, cung cấp cho lực lượng chuyên trách bảo vệ an ninh mạng thông tin, dữ liệu phục vụ bảo vệ an ninh mạng.

5. Chủ quản hệ thống thông tin quyết định việc bố trí lực lượng thường trực bảo vệ an ninh mạng; ban hành quy chế hoạt động; xác định nhiệm vụ,

quyền hạn, chế độ trực, trách nhiệm bảo mật và bảo đảm điều kiện hoạt động của lực lượng này theo quy định của pháp luật.

6. Khuyến khích tổ chức, doanh nghiệp cung cấp hạ tầng số, dịch vụ viễn thông, trung tâm dữ liệu, dịch vụ điện toán đám mây, dịch vụ an ninh mạng, dịch vụ tài chính, thanh toán, nền tảng số quy mô lớn hoặc xử lý khối lượng lớn dữ liệu cá nhân chủ động bố trí đơn vị hoặc bộ phận chuyên trách bảo vệ an ninh mạng đối với hệ thống thông tin, cơ sở dữ liệu thuộc phạm vi quản lý.

Điều 7. Lực lượng dự bị bảo vệ an ninh mạng

1. Lực lượng dự bị bảo vệ an ninh mạng là tổ chức, cá nhân có năng lực, kinh nghiệm, nhân lực, phương tiện, thiết bị, giải pháp kỹ thuật, sản phẩm, dịch vụ hoặc điều kiện phù hợp, được lập danh sách, quản lý, kết nối, phối hợp hoặc huy động tham gia bảo vệ an ninh mạng theo quy định tại điểm c khoản 1 Điều 30 Luật An ninh mạng.

2. Lực lượng dự bị bảo vệ an ninh mạng không phải là lực lượng chuyên trách, lực lượng thường trực hoặc lực lượng có tổ chức độc lập trong bộ máy nhà nước; không làm phát sinh biên chế, chức danh, cấp bậc, thẩm quyền công vụ hoặc quyền áp dụng biện pháp bảo vệ an ninh mạng.

3. Việc xây dựng, quản lý và huy động lực lượng dự bị bảo vệ an ninh mạng được thực hiện trên cơ sở tự nguyện, chương trình, kế hoạch, hợp đồng, thỏa thuận, đặt hàng, giao nhiệm vụ hoặc hình thức hợp pháp khác; bảo đảm đúng thẩm quyền, đúng mục đích, đúng phạm vi, phù hợp với năng lực của tổ chức, cá nhân được huy động và yêu cầu bảo vệ an ninh mạng.

4. Lực lượng dự bị bảo vệ an ninh mạng có thể được huy động tham gia một hoặc một số hoạt động sau đây:

a) Tư vấn, hỗ trợ kỹ thuật, nghiên cứu, phát triển giải pháp bảo vệ an ninh mạng;

b) Hỗ trợ kiểm tra, đánh giá, phát hiện, cảnh báo điểm yếu, lỗ hổng bảo mật, mã độc, nguy cơ mất an ninh mạng;

c) Hỗ trợ ứng phó, khắc phục sự cố an ninh mạng; phục hồi, phân tích dữ liệu điện tử, chứng cứ điện tử theo quy định của pháp luật;

d) Hỗ trợ đào tạo, bồi dưỡng, tập huấn kiến thức, kỹ năng bảo vệ an ninh mạng;

đ) Thực hiện nhiệm vụ khác phục vụ bảo vệ an ninh mạng theo quyết định, chương trình, kế hoạch, hợp đồng hoặc thỏa thuận hợp pháp với cơ quan, tổ chức có thẩm quyền.

5. Tổ chức, cá nhân thuộc lực lượng dự bị bảo vệ an ninh mạng có trách nhiệm:

a) Thực hiện đúng phạm vi, nội dung, thời hạn, phương thức và yêu cầu được giao, được đặt hàng, được thỏa thuận hoặc được cơ quan có thẩm quyền cho phép;

b) Tuân thủ quy định của pháp luật về bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân, bảo vệ bí mật kinh doanh, bí mật công tác và quyền, lợi ích hợp pháp của cơ quan, tổ chức, cá nhân có liên quan;

c) Không lợi dụng việc tham gia bảo vệ an ninh mạng để thu thập, khai thác, sử dụng, công bố, chia sẻ, mua bán, chuyển giao trái phép thông tin, dữ liệu, tài liệu, mã độc, điểm yếu, lỗ hổng bảo mật hoặc bí mật khác mà mình biết được trong quá trình tham gia;

d) Chịu trách nhiệm trước pháp luật về hành vi vi phạm trong quá trình tham gia bảo vệ an ninh mạng.

6. Trong trường hợp khẩn cấp để bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội trên không gian mạng, việc huy động chuyên gia, nhà khoa học, cán bộ chuyên sâu và trưng dụng hệ thống, phương tiện, thiết bị được thực hiện theo Điều 39 Luật An ninh mạng và quy định của pháp luật có liên quan.

7. Kinh phí, chi phí, thù lao, hỗ trợ hoặc chế độ khác đối với tổ chức, cá nhân thuộc lực lượng dự bị bảo vệ an ninh mạng được thực hiện theo chương trình, kế hoạch, hợp đồng, thỏa thuận, đặt hàng, giao nhiệm vụ, quyết định huy động, quyết định trưng dụng hoặc nguồn kinh phí hợp pháp khác theo quy định của pháp luật.

8. Bộ Công an chủ trì, phối hợp với Bộ Quốc phòng, Bộ Tài chính và cơ quan có liên quan hướng dẫn điều kiện, trình tự, thủ tục, phương thức xây dựng, quản lý, huy động và phối hợp lực lượng dự bị bảo vệ an ninh mạng; cơ chế quản lý, sử dụng, bảo mật thông tin; trách nhiệm của tổ chức, cá nhân được huy động; kinh phí, chi phí, thù lao, hỗ trợ và các nội dung cần thiết khác theo quy định của pháp luật.

Điều 8. Tiêu chuẩn đối với cá nhân tham gia lực lượng bảo vệ an ninh mạng

1. Cá nhân tham gia lực lượng chuyên trách bảo vệ an ninh mạng và lực lượng thường trực bảo vệ an ninh mạng bố trí tại bộ, ngành, Ủy ban nhân dân cấp tỉnh, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia phải bảo đảm tiêu chuẩn theo quy định của Luật An ninh mạng, quy định pháp luật có liên quan và các tiêu chuẩn sau:

a) Tiêu chuẩn chuyên môn theo vị trí việc làm bao gồm khung năng lực, yêu cầu về văn bằng, chứng chỉ chuyên môn, kỹ năng, kinh nghiệm và sản phẩm công việc theo quy định của cơ quan có thẩm quyền;

b) Đối với vị trí tiếp cận hệ thống thông tin quan trọng, dữ liệu nhạy cảm hoặc thực hiện điều tra số, cơ quan quản lý thực hiện thẩm định độ tin cậy, kiểm soát xung đột lợi ích và quản trị truy cập theo nguyên tắc tối thiểu.

2. Cá nhân tham gia lực lượng dự bị và lực lượng thường trực bảo vệ an ninh mạng không thuộc quy định tại khoản 1 Điều này đáp ứng các tiêu chuẩn sau đây:

a) Có phẩm chất chính trị, đạo đức, ý thức kỷ luật phù hợp với yêu cầu nhiệm vụ;

b) Không thuộc trường hợp có xung đột lợi ích theo quy định của pháp luật;

c) Có năng lực chuyên môn phù hợp với nhiệm vụ được giao;

d) Có ý thức tuân thủ các quy định, cam kết về bảo vệ bí mật nhà nước, bí mật công tác, bảo mật thông tin.

3. Bộ Công an chủ trì, phối hợp với Bộ Quốc phòng và cơ quan có liên quan ban hành theo thẩm quyền hoặc trình cấp có thẩm quyền ban hành quy định về khung năng lực, tiêu chuẩn vị trí việc làm, tiêu chí đánh giá kết quả thực hiện nhiệm vụ, quy trình thẩm định độ tin cậy và kiểm soát xung đột lợi ích đối với lực lượng bảo vệ an ninh mạng.

Điều 9. Phối hợp giữa các lực lượng bảo vệ an ninh mạng

1. Việc phối hợp trong bảo vệ an ninh mạng phải bảo đảm nguyên tắc sau:

a) Kịp thời, hiệu quả, đúng chức năng, nhiệm vụ, thẩm quyền; chia sẻ thông tin có kiểm soát, đúng mục đích, đúng đối tượng; không làm gián đoạn trái pháp luật hoạt động bình thường của cơ quan, tổ chức, doanh nghiệp;

b) Thực hiện trên cơ sở quy định của pháp luật, hợp đồng, thỏa thuận; xác định rõ trách nhiệm của các bên, phạm vi chia sẻ dữ liệu, yêu cầu bảo mật và cơ chế xử lý rủi ro theo quy định của pháp luật.

2. Nội dung phối hợp bao gồm:

a) Trao đổi, cung cấp thông tin, dữ liệu phục vụ phối hợp bảo vệ an ninh mạng;

b) Tham gia xử lý tình huống nguy hiểm về an ninh mạng; ứng cứu, khắc phục sự cố an ninh mạng;

c) Triển khai các biện pháp bảo vệ an ninh mạng theo quy định của pháp luật;

d) Đào tạo, tập huấn, diễn tập, nghiên cứu, thử nghiệm trong bảo vệ an ninh mạng;

đ) Hoạt động khác phục vụ trực tiếp bảo vệ an ninh mạng, an ninh dữ liệu.

3. Việc phối hợp giữa lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an và Bộ Quốc phòng được thực hiện trên nguyên tắc chủ động, hiệp đồng, phân công rõ ràng, không chồng chéo chức năng, nhiệm vụ, bảo đảm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng, cụ thể như sau:

a) Lực lượng chuyên trách thuộc Bộ Công an là lực lượng nòng cốt, chủ trì triển khai công tác bảo vệ an ninh mạng trên phạm vi toàn quốc; chủ trì, phối hợp với cơ quan, tổ chức có liên quan trong phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi vi phạm pháp luật trên không gian mạng và bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia (trừ hệ thống thông tin quân sự và hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ theo quy định của pháp luật);

b) Lực lượng chuyên trách thuộc Bộ Quốc phòng chủ trì bảo vệ an ninh mạng đối với hệ thống thông tin quân sự; phát hiện, ngăn chặn, xử lý theo thẩm quyền các hành vi vi phạm pháp luật về an ninh mạng đối với hệ thống thông tin quân sự.

4. Hình thức và nội dung phối hợp giữa các lực lượng bảo vệ an ninh mạng được thực hiện như sau:

a) Phối hợp theo yêu cầu được thực hiện khi có yêu cầu, chỉ đạo của cơ quan có thẩm quyền hoặc theo đề nghị của cơ quan chủ trì, bao gồm: ứng phó, xử lý tấn công mạng, khủng bố mạng, sự cố an ninh mạng; bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia; điều tra, xử lý hành vi vi phạm pháp luật trên không gian mạng; tổ chức diễn tập phòng thủ không gian mạng;

b) Phối hợp không theo yêu cầu được thực hiện trên cơ sở trao đổi, chia sẻ thông tin, dữ liệu và hiệp đồng tác chiến, bao gồm: chia sẻ thông tin về nguy cơ, tình huống tấn công mạng, khủng bố mạng, sự cố an ninh mạng; phối hợp phòng ngừa, phát hiện, ngăn chặn, điều tra, xử lý hành vi vi phạm pháp luật trên không gian mạng; bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia; tổ chức diễn tập, huấn luyện phòng thủ không gian mạng.

5. Bộ Công an chủ trì thiết lập và duy trì cơ chế, hệ thống điều phối chung giữa các lực lượng bảo vệ an ninh mạng; việc tiếp nhận, xác thực thông tin, điều phối ứng cứu sự cố được thực hiện trên nguyên tắc không làm thay đổi thẩm quyền quản lý, vận hành, xử lý của Bộ Quốc phòng đối với hệ thống thông tin quân sự và Ban Cơ yếu Chính phủ đối với hệ thống thông tin cơ yếu; cơ quan, tổ chức, doanh nghiệp có hệ thống thông tin quan trọng có trách nhiệm công bố đầu mối liên hệ 24/7 để phối hợp.

Điều 10. Trao đổi, cung cấp thông tin, dữ liệu phục vụ phối hợp bảo vệ an ninh mạng

1. Thông tin, dữ liệu chia sẻ bao gồm nhật ký kỹ thuật; thông tin, dữ liệu kỹ thuật phản ánh dấu hiệu, đặc điểm, phương thức, thủ đoạn tấn công mạng hoặc hành vi khác xâm phạm an ninh mạng; mẫu mã độc; khuyến nghị cấu

hình; thông tin rủi ro; biện pháp khắc phục và dữ liệu cần thiết khác phục vụ trực tiếp hoạt động bảo vệ an ninh mạng.

2. Việc trao đổi, cung cấp thông tin, dữ liệu trong phối hợp lực lượng bảo vệ an ninh mạng phải bảo đảm tuân thủ quy định của pháp luật về bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân, bảo vệ bí mật kinh doanh và quy định khác của pháp luật có liên quan, đúng mục đích, phân loại mức độ nhạy cảm, bảo mật, lưu vết và không tái phân phối trái phép.

3. Cơ quan, tổ chức, cá nhân nhận thông tin, dữ liệu có trách nhiệm sử dụng đúng mục đích, áp dụng biện pháp bảo mật, lưu vết và thực hiện yêu cầu của cơ quan điều phối hoặc chủ thể cung cấp dữ liệu.

4. Hình thức trao đổi, cung cấp thông tin, dữ liệu bao gồm văn bản, điện thoại, phương thức điện tử hoặc hình thức khác theo quy định của pháp luật.

5. Bộ Công an thiết lập, quản lý cổng kết nối trực tuyến phục vụ trao đổi, cung cấp thông tin, dữ liệu phục vụ phối hợp bảo vệ an ninh mạng.

6. Việc trao đổi, cung cấp thông tin, dữ liệu liên quan đến thông tin quân sự, hệ thống thông tin quân sự của Bộ Quốc phòng, hệ thống thông tin cơ yếu của Ban Cơ yếu Chính phủ tuân thủ pháp luật về bảo vệ bí mật nhà nước, pháp luật về cơ yếu, pháp luật về quốc phòng và quy định chuyên ngành có liên quan, đồng thời bảo đảm yêu cầu phối hợp, chia sẻ thông tin phục vụ bảo vệ an ninh mạng.

Điều 11. Huy động và khuyến khích tổ chức, cá nhân tham gia bảo vệ an ninh mạng

1. Việc huy động, khuyến khích tổ chức, cá nhân tham gia bảo vệ an ninh mạng được thực hiện trong các trường hợp sau đây:

a) Xử lý tình huống khẩn cấp, nghiêm trọng về an ninh mạng; tình huống nguy hiểm về an ninh mạng có nguy cơ ảnh hưởng đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân;

b) Bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia; hệ thống thông tin, cơ sở dữ liệu, hạ tầng số, nền tảng số có vai trò trọng yếu, thiết yếu đối với hoạt động của cơ quan nhà nước, quốc phòng, an ninh, kinh tế - xã hội;

c) Phòng ngừa, phát hiện, ngăn chặn, xử lý mã độc, lỗ hổng bảo mật, điểm yếu kỹ thuật, nguy cơ tấn công mạng, sự cố an ninh mạng và các hành vi xâm phạm an ninh mạng;

d) Bảo vệ bí mật nhà nước, bí mật công tác, bí mật kinh doanh, dữ liệu cá nhân, dữ liệu cá nhân nhạy cảm, dữ liệu quan trọng và dữ liệu khác cần được bảo vệ theo quy định của pháp luật;

đ) Phòng, chống khủng bố mạng, gián điệp mạng, tấn công mạng, phá hoại hệ thống thông tin, xâm hại trẻ em trên không gian mạng và các hành vi sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội;

e) Huấn luyện, diễn tập, kiểm tra, đánh giá an ninh mạng; thử nghiệm, rà quét, đánh giá lỗ hổng, kiểm thử xâm nhập, đánh giá khả năng ứng phó, phục hồi của hệ thống thông tin theo chương trình, kế hoạch, hợp đồng, thỏa thuận hoặc yêu cầu của cơ quan có thẩm quyền;

g) Thực hiện nhiệm vụ chuyên môn khác phục vụ trực tiếp hoạt động bảo vệ an ninh mạng theo quyết định, yêu cầu hoặc văn bản giao nhiệm vụ của cơ quan có thẩm quyền.

2. Việc huy động, khuyến khích tổ chức, cá nhân tham gia bảo vệ an ninh mạng quy định tại khoản 1 Điều này phải bảo đảm đúng thẩm quyền, đúng mục đích, đúng phạm vi, có thời hạn, có yêu cầu bảo mật, chế độ báo cáo và trách nhiệm cụ thể theo quy định của pháp luật.

3. Hình thức tham gia bảo vệ an ninh mạng

a) Huy động thông qua quyết định của cơ quan, người có thẩm quyền;

b) Hợp đồng, thỏa thuận, đặt hàng, giao nhiệm vụ, cơ chế cộng đồng hoặc hình thức hợp pháp khác theo quy định của pháp luật;

c) Qua nền tảng kết nối tham gia bảo vệ an ninh mạng quy định tại khoản 8 Điều này.

4. Thẩm quyền huy động

a) Bộ trưởng Bộ Công an quyết định hoặc ủy quyền việc ban hành quyết định theo quy định tại điểm a khoản 3 Điều này, trường hợp cần huy động đơn vị thuộc Bộ Quốc phòng có hoạt động dân sự, kinh tế, Bộ trưởng Bộ Công an trao đổi thống nhất với Bộ trưởng Bộ Quốc phòng trước khi quyết định huy động theo quy định tại Nghị định này, trừ trường hợp quy định tại điểm b khoản 4 Điều này;

b) Bộ trưởng Bộ Quốc phòng quyết định hoặc ủy quyền việc ban hành quyết định theo quy định tại điểm a khoản 3 Điều này để phục vụ nhiệm vụ quân sự, quốc phòng;

c) Lực lượng chuyên trách bảo vệ an ninh mạng huy động tổ chức, cá nhân tham gia bảo vệ an ninh mạng theo quy định tại điểm b hoặc điểm c khoản 3 Điều này.

5. Quyết định huy động phải xác định rõ căn cứ huy động, mục tiêu, phạm vi, nhiệm vụ, tổ chức, cá nhân tham gia, thời gian, thời hạn, yêu cầu bảo mật, chế độ báo cáo, nghĩa vụ, trách nhiệm có liên quan.

6. Chủ quản hệ thống thông tin hợp tác với tổ chức, cá nhân tham gia bảo vệ an ninh mạng theo quy định tại điểm b hoặc điểm c khoản 3 Điều này đối với hệ thống thông tin, cơ sở dữ liệu thuộc phạm vi quản lý theo nguyên tắc tự nguyện, bình đẳng, phối hợp, chia sẻ thông tin, hỗ trợ kỹ thuật và tuân thủ quy định của pháp luật.

7. Hợp tác tự nguyện tham gia bảo vệ an ninh mạng

a) Khuyến khích cơ quan, tổ chức, doanh nghiệp, tổ chức xã hội nghề nghiệp, cơ sở nghiên cứu, cơ sở đào tạo, chuyên gia và cá nhân có năng lực chuyên môn hình thành mạng lưới, liên minh tham gia bảo vệ an ninh mạng theo nguyên tắc tự nguyện, bình đẳng, phối hợp, chia sẻ thông tin, hỗ trợ kỹ thuật và tuân thủ quy định của pháp luật;

b) Mạng lưới, liên minh tham gia bảo vệ an ninh mạng được tổ chức theo ngành, lĩnh vực, địa bàn, khu vực, nhóm hệ thống thông tin, chuỗi cung ứng số, hạ tầng số hoặc theo chuyên đề, chuyên môn kỹ thuật, mục tiêu hỗ trợ bảo vệ an ninh mạng cụ thể;

c) Quy chế hoạt động hoặc thỏa thuận tham gia mạng lưới, liên minh bảo vệ an ninh mạng phải xác định tối thiểu mục tiêu, phạm vi hoạt động; thành viên, điều kiện tham gia, chấm dứt tham gia; đầu mối điều phối; cơ chế phối hợp và chia sẻ thông tin; nguyên tắc bảo mật; cơ chế huy động nguồn lực, hỗ trợ kỹ thuật, huấn luyện, diễn tập, cảnh báo và giải quyết vướng mắc.

8. Nền tảng kết nối tham gia bảo vệ an ninh mạng

a) Nền tảng kết nối là sản phẩm, dịch vụ công nghệ thông tin hỗ trợ liên kết, chia sẻ thông tin, dữ liệu, phối hợp hành động, phân phối nhiệm vụ, kết nối chuyên gia, huy động cộng đồng trên không gian mạng tham gia nhiệm vụ bảo vệ an ninh mạng, an ninh dữ liệu;

b) Tổ chức, doanh nghiệp cung cấp nền tảng kết nối tham gia bảo vệ an ninh mạng phải có giấy phép kinh doanh dịch vụ an ninh mạng.

9. Tổ chức, doanh nghiệp, cá nhân được huy động tham gia bảo vệ an ninh mạng theo nhiệm vụ cụ thể, trong thời hạn xác định và được bảo đảm quyền, lợi ích hợp pháp.

Điều 12. Huy động, phối hợp lực lượng bảo vệ an ninh mạng tham gia săn tìm, phát hiện và báo cáo điểm yếu, lỗ hổng bảo mật

1. Khuyến khích lực lượng bảo vệ an ninh mạng, cơ quan, tổ chức, doanh nghiệp chủ quản hệ thống thông tin thiết lập cơ chế, chương trình, kế hoạch hoặc hoạt động săn tìm, phát hiện, xác minh, phân loại, báo cáo và điều phối xử lý điểm yếu, lỗ hổng bảo mật đối với hệ thống thông tin, cơ sở dữ liệu, nền tảng số thuộc phạm vi quản lý theo quy định của pháp luật.

2. Việc huy động, phối hợp lực lượng bảo vệ an ninh mạng, tổ chức, cá nhân có năng lực phù hợp tham gia săn tìm, phát hiện và báo cáo điểm yếu, lỗ hổng bảo mật chỉ được thực hiện trong phạm vi hệ thống thông tin, cơ sở dữ liệu, nền tảng số được cơ quan, tổ chức, doanh nghiệp chủ quản cho phép theo chương trình, kế hoạch, hợp đồng, thỏa thuận, đặt hàng, giao nhiệm vụ hoặc hình thức hợp pháp khác.

3. Việc công bố chương trình săn tìm, phát hiện và báo cáo điểm yếu, lỗ hổng bảo mật được thực hiện thông qua nền tảng quy định tại khoản 8 Điều 11 Nghị định này, thông qua dịch vụ an ninh mạng theo quy định của pháp luật hoặc thông qua hình thức công bố chính thức khác của cơ quan, tổ chức, doanh nghiệp chủ quản hệ thống thông tin.

4. Tổ chức, cá nhân tham gia săn tìm, phát hiện và báo cáo điểm yếu, lỗ hổng bảo mật có trách nhiệm:

a) Thực hiện đúng phạm vi, thời hạn, phương thức và yêu cầu kỹ thuật được cơ quan, tổ chức, doanh nghiệp chủ quản hệ thống thông tin cho phép;

b) Không công bố, chia sẻ, mua bán, chuyển giao trái phép thông tin về điểm yếu, lỗ hổng bảo mật;

c) Không khai thác vượt quá mức cần thiết để chứng minh sự tồn tại của điểm yếu, lỗ hổng bảo mật;

d) Không làm gián đoạn, cản trở, phá hoại hoặc gây ảnh hưởng đến hoạt động bình thường của hệ thống thông tin, cơ sở dữ liệu, nền tảng số;

đ) Tuân thủ quy định của pháp luật về bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân, bảo vệ bí mật kinh doanh, bảo vệ quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân có liên quan.

5. Cơ quan, tổ chức, doanh nghiệp chủ quản hệ thống thông tin có trách nhiệm:

a) Xác định rõ phạm vi, điều kiện, phương thức, yêu cầu kỹ thuật và giới hạn được phép săn tìm, phát hiện điểm yếu, lỗ hổng bảo mật trong chương trình, kế hoạch, hợp đồng, thỏa thuận, đặt hàng hoặc giao nhiệm vụ;

b) Tiếp nhận, xác minh, phân loại, xử lý hoặc phối hợp xử lý thông tin về điểm yếu, lỗ hổng bảo mật được báo cáo;

c) Áp dụng kịp thời biện pháp khắc phục đối với điểm yếu, lỗ hổng bảo mật đã được xác minh;

d) Bảo mật thông tin về tổ chức, cá nhân báo cáo điểm yếu, lỗ hổng bảo mật theo quy định của pháp luật;

đ) Báo cáo lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an trong trường hợp điểm yếu, lỗ hổng bảo mật có khả năng ảnh hưởng đến an ninh quốc gia, trật tự, an toàn xã hội, hệ thống thông tin quan trọng về an ninh quốc gia, dữ liệu quan trọng hoặc dữ liệu cá nhân theo quy định của pháp luật.

6. Cơ quan, tổ chức, doanh nghiệp, cá nhân khi phát hiện điểm yếu, lỗ hổng bảo mật của hệ thống thông tin, cơ sở dữ liệu, nền tảng số không thuộc phạm vi quản lý hoặc không thuộc phạm vi được cho phép săn tìm, phát hiện có trách nhiệm thông báo cho chủ quản hệ thống thông tin, lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an hoặc cơ quan có thẩm quyền khác theo quy định của pháp luật; không được tự ý khai thác, công bố, chia sẻ, mua bán, chuyển giao thông tin về điểm yếu, lỗ hổng bảo mật.

7. Việc ghi nhận kết quả, chi trả thù lao, hỗ trợ chi phí hoặc tiền thưởng cho tổ chức, cá nhân phát hiện, báo cáo điểm yếu, lỗ hổng bảo mật được thực hiện trên cơ sở chương trình, kế hoạch, hợp đồng, thỏa thuận, đặt hàng, giao nhiệm vụ hoặc nguồn kinh phí hợp pháp khác; bảo đảm đúng thẩm quyền, đúng đối tượng, đúng nội dung chi, công khai, minh bạch và phù hợp với quy định của pháp luật.

8. Bộ Công an chủ trì, phối hợp với Bộ Quốc phòng, Bộ Tài chính và cơ quan có liên quan hướng dẫn điều kiện, quy trình, thủ tục huy động, phối hợp lực lượng bảo vệ an ninh mạng tham gia săn tìm, phát hiện và báo cáo điểm yếu, lỗ hổng bảo mật; việc tiếp nhận, xác minh, phân loại, lưu vết, bảo toàn dữ liệu, báo cáo, xử lý, khắc phục lỗ hổng bảo mật; việc ghi nhận kết quả, hỗ trợ chi phí, chi trả thù lao hoặc tiền thưởng theo quy định của pháp luật.

Chương III
CHÍNH SÁCH ĐÃI NGỘ, THU HÚT NHÂN TÀI ĐỐI VỚI LỰC LƯỢNG CHUYÊN TRÁCH BẢO VỆ AN NINH MẠNG

Điều 13. Nguyên tắc áp dụng chính sách đãi ngộ, thu hút nhân tài trong lực lượng chuyên trách bảo vệ an ninh mạng

1. Chính sách đãi ngộ, thu hút nhân tài trong lực lượng chuyên trách bảo vệ an ninh mạng được áp dụng đối với các đối tượng quy định tại Nghị định này, bao gồm:

a) Người đang thuộc lực lượng chuyên trách bảo vệ an ninh mạng;

b) Người chưa thuộc lực lượng chuyên trách bảo vệ an ninh mạng nhưng được xem xét tuyển dụng, tiếp nhận, bố trí, sử dụng hoặc ký hợp đồng để tham gia thực hiện nhiệm vụ trong lực lượng chuyên trách bảo vệ an ninh mạng.

2. Việc áp dụng tiền lương, tiền công, thù lao, hỗ trợ tăng thêm, thu nhập và chính sách khác đối với từng đối tượng được thực hiện theo hình thức tuyển

dụng, tiếp nhận, bố trí, sử dụng hoặc ký kết hợp đồng, bảo đảm không trùng lặp chế độ, chính sách và phù hợp với nguồn kinh phí hợp pháp.

3. Việc áp dụng chính sách phải bảo đảm các nguyên tắc sau đây:

a) Đúng đối tượng, đúng tiêu chí, tiêu chuẩn, điều kiện, đúng thẩm quyền và đúng quy định của pháp luật;

b) Phù hợp với vị trí việc làm, chức danh, chức vụ, tính chất nhiệm vụ, mức độ cống hiến, kết quả thực hiện nhiệm vụ và yêu cầu xây dựng, phát triển lực lượng chuyên trách bảo vệ an ninh mạng;

c) Công khai, minh bạch, khách quan, công bằng, hiệu quả;

d) Gắn với yêu cầu bảo vệ bí mật nhà nước, bảo đảm an ninh mạng, an ninh dữ liệu, an ninh thông tin mạng và yêu cầu bảo vệ chính trị nội bộ.

4. Việc tiếp tục áp dụng, điều chỉnh, gia hạn, tạm dừng hoặc chấm dứt áp dụng chính sách được thực hiện trên cơ sở kết quả rà soát, đánh giá định kỳ hoặc khi có thay đổi về vị trí việc làm, nhiệm vụ được giao, tổ chức bộ máy, biên chế hoặc điều kiện áp dụng chính sách.

5. Không áp dụng hoặc chấm dứt áp dụng chính sách quy định tại Chương này đối với trường hợp không còn đáp ứng tiêu chí, tiêu chuẩn, điều kiện; vi phạm pháp luật; vi phạm quy định về bảo vệ bí mật nhà nước, bảo đảm an ninh mạng, an ninh dữ liệu, an ninh thông tin mạng; hoặc đang bị xem xét xử lý kỷ luật, đang chấp hành hình thức kỷ luật, trừ trường hợp pháp luật có quy định khác.

Điều 14. Tiêu chí, tiêu chuẩn, điều kiện áp dụng chính sách đãi ngộ đối với lực lượng chuyên trách bảo vệ an ninh mạng

1. Đối tượng áp dụng chính sách đãi ngộ theo Điều này là người đang thuộc lực lượng chuyên trách bảo vệ an ninh mạng và đáp ứng các tiêu chí, tiêu chuẩn, điều kiện sau đây:

a) Được cơ quan có thẩm quyền tuyển dụng, tiếp nhận, bố trí vào biên chế, vị trí việc làm, chức danh, chức vụ hoặc giao nhiệm vụ trong lực lượng chuyên trách bảo vệ an ninh mạng;

b) Có phẩm chất chính trị, đạo đức, ý thức tổ chức kỷ luật, trách nhiệm nghề nghiệp đáp ứng yêu cầu nhiệm vụ;

c) Có trình độ chuyên môn, nghiệp vụ, kỹ năng phù hợp với lĩnh vực an ninh mạng, an ninh thông tin mạng, công nghệ thông tin, điện tử, viễn thông, mật mã, điều tra số, pháp y số, ứng cứu sự cố mạng, phân tích mã độc, nghiên cứu lỗ hổng bảo mật, bảo đảm an ninh dữ liệu hoặc lĩnh vực công nghệ cao khác có liên quan trực tiếp;

d) Trực tiếp thực hiện nhiệm vụ bảo vệ an ninh mạng theo quy định tại khoản 2 Điều 5 Nghị định này.

2. Việc xác định mức đãi ngộ đối với đối tượng quy định tại khoản 1 Điều này phải gắn với tính chất nhiệm vụ, cường độ công việc, mức độ phức tạp về kỹ thuật, yêu cầu trực sẵn sàng, ứng cứu, xử lý khẩn cấp và yêu cầu bảo mật đặc biệt.

3. Chính sách đãi ngộ theo Điều này không áp dụng đối với người chưa thuộc lực lượng chuyên trách bảo vệ an ninh mạng và đang được xem xét áp dụng chính sách thu hút nhân tài quy định tại Điều 15 của Nghị định này.

Điều 15. Tiêu chí, tiêu chuẩn, điều kiện áp dụng chính sách thu hút nhân tài vào lực lượng chuyên trách bảo vệ an ninh mạng

1. Đối tượng áp dụng chính sách thu hút nhân tài theo Điều này là người chưa thuộc lực lượng chuyên trách bảo vệ an ninh mạng, được xem xét tuyển dụng, tiếp nhận, bố trí, sử dụng hoặc ký hợp đồng để tham gia thực hiện nhiệm vụ trong lực lượng chuyên trách bảo vệ an ninh mạng, khi đáp ứng một trong các tiêu chí, tiêu chuẩn, điều kiện sau đây:

a) Là chuyên gia, nhà khoa học, kỹ sư, lập trình viên, chuyên gia dữ liệu, chuyên gia trí tuệ nhân tạo, chuyên gia mật mã, chuyên gia điện tử - viễn thông, chuyên gia bán dẫn, chuyên gia công nghệ lượng tử, chuyên gia phân tích mã độc, chuyên gia điều tra số, chuyên gia ứng cứu sự cố mạng hoặc người có trình độ chuyên môn cao trong lĩnh vực có liên quan trực tiếp đến bảo vệ an ninh mạng;

b) Có công trình nghiên cứu, sáng chế, giải pháp, sản phẩm, phần mềm, nền tảng, mô hình, kết quả thực tiễn hoặc thành tích nghề nghiệp được cơ quan, tổ chức có thẩm quyền hoặc giới chuyên môn trong nước, quốc tế ghi nhận;

c) Là sinh viên tốt nghiệp hạng xuất sắc, nhà khoa học trẻ, kỹ sư trẻ tài năng, người có thành tích đặc biệt xuất sắc trong học tập, nghiên cứu, thi đấu, sáng tạo, phát triển công nghệ thuộc ngành, chuyên ngành phù hợp;

d) Có thành tích đặc biệt xuất sắc, vượt trội so với yêu cầu của vị trí dự kiến bố trí hoặc có sáng kiến, giải pháp đột phá, tạo ra sản phẩm, kết quả cụ thể có giá trị cao, đóng góp thiết thực cho công tác bảo vệ an ninh mạng;

đ) Có uy tín chuyên môn, kinh nghiệm thực tiễn nổi trội, có khả năng giải quyết các vấn đề phức tạp, mới, khó, cấp bách trong lĩnh vực an ninh mạng.

2. Việc áp dụng chính sách thu hút nhân tài phải bảo đảm đúng đối tượng, đúng tiêu chuẩn, đúng thẩm quyền, công khai, minh bạch, khách quan, hiệu quả và gắn với yêu cầu xây dựng, phát triển lực lượng chuyên trách bảo vệ an ninh mạng.

3. Người được xem xét áp dụng chính sách thu hút nhân tài theo Điều này chỉ được áp dụng chính sách đãi ngộ quy định tại Điều 16 của Nghị định này sau khi đã được tuyển dụng, tiếp nhận, bố trí hoặc giao nhiệm vụ trong lực lượng chuyên trách bảo vệ an ninh mạng theo quy định của pháp luật.

Điều 16. Chính sách tiền lương, tiền công, thù lao và hỗ trợ tăng thêm hằng tháng

1. Người được tuyển chọn, tiếp nhận, bố trí, sử dụng, giao nhiệm vụ hoặc ký kết hợp đồng để thực hiện nhiệm vụ trong lực lượng chuyên trách bảo vệ an ninh mạng được hưởng tiền lương, tiền công, thù lao, phụ cấp, hỗ trợ và chế độ khác theo quy định của pháp luật, phù hợp với hình thức sử dụng, vị trí việc làm, chức danh, chức vụ, tính chất nhiệm vụ và kết quả thực hiện nhiệm vụ.

2. Người thuộc biên chế lực lượng chuyên trách bảo vệ an ninh mạng hoặc thuộc diện đãi ngộ, thu hút nhân tài, ngoài chế độ tiền lương, phụ cấp và chế độ khác theo quy định của pháp luật, được xem xét hưởng hỗ trợ tăng thêm hằng tháng theo một trong các mức sau đây:

a) Mức 1, tối đa bằng 100% mức lương theo hệ số lương hiện hưởng đối với trường hợp thực hiện nhiệm vụ chuyên môn, nghiệp vụ trong lực lượng chuyên trách bảo vệ an ninh mạng, có yêu cầu về trình độ, chuyên môn và kết quả công việc không thuộc diện quy định tại điểm b và điểm c khoản này;

b) Mức 2, tối đa bằng 200% mức lương theo hệ số lương hiện hưởng đối với người trực tiếp thực hiện những nhiệm vụ trong lĩnh vực tham mưu chiến lược về bảo vệ an ninh mạng hoặc dự án công nghệ chiến lược; trực tiếp thực hiện nhiệm vụ yêu cầu trình độ chuyên môn, nghiệp vụ chuyên sâu, tổ chức công tác huấn luyện, đào tạo bảo vệ an ninh mạng; trực tiếp đấu tranh phòng, chống hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia, phòng chống gián điệp mạng, khủng bố mạng, chiến tranh mạng, tội phạm mạng; xây dựng, triển khai quy trình nghiệp vụ quan trọng có yêu cầu bảo mật, kỹ thuật cao; nghiên cứu, phát triển, vận hành, bảo vệ hệ thống, nền tảng, công cụ, giải pháp công nghệ chiến lược phục vụ bảo vệ an ninh mạng, giám sát, phân tích, đánh giá, cảnh báo sớm các nguy cơ đe dọa an ninh mạng quốc gia; thực hiện nhiệm vụ có cường độ cao, trực sẵn sàng, xử lý khẩn cấp phục vụ bảo vệ an ninh mạng; tổ chức thực hiện nhiệm vụ bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia, bảo đảm an ninh dữ liệu, an ninh thông tin mạng; hoặc có sản phẩm đầu ra phục vụ trực tiếp công tác quản lý, chỉ đạo, điều hành, tác chiến, bảo vệ an ninh mạng;

c) Mức 3, tối đa bằng 300% mức lương theo hệ số lương hiện hưởng đối với người trực tiếp nghiên cứu, phát triển, làm chủ ứng dụng công nghệ chiến

lược, sản phẩm công nghệ chiến lược hoặc công nghệ mới có tác động trực tiếp đến an ninh quốc gia; trực tiếp nghiên cứu, phát triển sản phẩm, giải pháp công nghệ, mô hình, đề án, dự án chiến lược có giá trị đột phá đối với bảo vệ an ninh mạng; thực hiện nhiệm vụ có yêu cầu bảo mật đặc biệt, cường độ đặc biệt cao, tự chủ ứng dụng, xử lý tình huống khẩn cấp 24/7 hoặc nhiệm vụ có ảnh hưởng lớn đến an ninh quốc gia, trật tự, an toàn xã hội.

3. Trường hợp người được hưởng hỗ trợ tăng thêm hằng tháng không áp dụng chế độ tiền lương theo hệ số lương hoặc pháp luật về tiền lương thay đổi căn cứ tính lương, mức hỗ trợ được xác định theo căn cứ tương ứng phù hợp với quy định của pháp luật về tiền lương, ngân sách nhà nước.

4. Người không thuộc biên chế nhưng được bố trí, sử dụng, giao nhiệm vụ hoặc ký kết hợp đồng để thực hiện nhiệm vụ trong lực lượng chuyên trách bảo vệ an ninh mạng được hưởng tiền công, thù lao, hỗ trợ chi phí trực tiếp, hợp lý, cần thiết và chế độ khác phù hợp với trình độ chuyên môn, tính chất nhiệm vụ, mức độ đóng góp, kết quả thực hiện nhiệm vụ, theo thỏa thuận, hợp đồng, quyết định giao nhiệm vụ hoặc quyết định của cơ quan có thẩm quyền.

5. Việc áp dụng chính sách quy định tại Điều này phải bảo đảm đúng đối tượng, đúng điều kiện, đúng thẩm quyền, phù hợp với vị trí việc làm, chức danh, chức vụ, tính chất nhiệm vụ, mức độ cống hiến và kết quả thực hiện nhiệm vụ; phù hợp với khả năng cân đối ngân sách nhà nước và nguồn kinh phí hợp pháp khác theo quy định của pháp luật.

6. Trường hợp một người đồng thời đáp ứng điều kiện hưởng nhiều mức hỗ trợ tăng thêm hằng tháng hoặc nhiều chính sách hỗ trợ, đãi ngộ có cùng tính chất, mục đích thì chỉ được hưởng một mức cao nhất, trừ trường hợp pháp luật có quy định khác.

7. Khoản hỗ trợ hằng tháng quy định tại khoản 2 Điều này được trả cùng kỳ lương; không dùng làm căn cứ để tính đóng, hưởng chế độ bảo hiểm xã hội và được miễn thuế thu nhập cá nhân cùng các nghĩa vụ tài chính khác đối với Nhà nước.

8. Kinh phí thực hiện chính sách quy định tại Điều này được bảo đảm từ ngân sách nhà nước trong phạm vi dự toán được cấp có thẩm quyền giao và nguồn kinh phí hợp pháp khác theo quy định của pháp luật. Việc lập dự toán, phân bổ, quản lý, sử dụng, thanh toán, quyết toán kinh phí thực hiện theo quy định của pháp luật về ngân sách nhà nước và pháp luật có liên quan.

9. Bộ trưởng Bộ Công an, Bộ trưởng Bộ Quốc phòng, trong phạm vi chức năng, nhiệm vụ, quyền hạn của mình, chủ trì, phối hợp với Bộ Tài chính và cơ

quan có liên quan quy định hoặc hướng dẫn tiêu chí xác định đối tượng, nhóm vị trí việc làm, mức hỗ trợ, thời gian hưởng, nguồn kinh phí, trình tự, thủ tục, thẩm quyền quyết định, cơ chế rà soát, kiểm tra, đánh giá, thanh toán và quyết toán việc thực hiện chính sách quy định tại Điều này.

Điều 17. Chính sách đào tạo, bồi dưỡng, sử dụng và phát triển

1. Đối tượng thuộc diện đãi ngộ, thu hút nhân tài trong lực lượng chuyên trách bảo vệ an ninh mạng được ưu tiên đào tạo, bồi dưỡng, cập nhật kiến thức, nâng cao trình độ chuyên môn, kỹ năng nghiệp vụ, năng lực quản lý, chỉ huy, nghiên cứu, phát triển và hợp tác quốc tế phù hợp với yêu cầu nhiệm vụ.

2. Căn cứ phẩm chất, năng lực, trình độ, kết quả thực hiện nhiệm vụ và yêu cầu xây dựng lực lượng, đối tượng thuộc diện đãi ngộ, thu hút nhân tài được xem xét bố trí, sử dụng vào vị trí việc làm phù hợp; được quy hoạch, bổ nhiệm, giao nhiệm vụ, giao đề án, giao nhiệm vụ trọng điểm, biệt phái, luân chuyển hoặc tạo điều kiện phát triển nghề nghiệp theo quy định của pháp luật.

3. Đối tượng có thành tích đặc biệt xuất sắc, năng lực nổi trội, có sản phẩm, công trình hoặc kết quả công tác có giá trị cao được ưu tiên xem xét đưa vào diện trọng dụng, giao nhiệm vụ quan trọng, chiến lược hoặc xem xét tiếp tục áp dụng cơ chế, chính sách phù hợp theo quy định của pháp luật.

4. Việc đào tạo, bồi dưỡng, sử dụng và phát triển phải bảo đảm đúng mục tiêu, đúng đối tượng, hiệu quả, thiết thực, gắn với yêu cầu nhiệm vụ, vị trí việc làm và định hướng xây dựng nguồn nhân lực chất lượng cao trong lực lượng chuyên trách bảo vệ an ninh mạng.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 18. Kinh phí thực hiện

1. Kinh phí thực hiện Nghị định được bảo đảm từ ngân sách nhà nước theo phân cấp ngân sách hiện hành, trong dự toán hằng năm của cơ quan, đơn vị được giao nhiệm vụ; vốn đầu tư công theo kế hoạch được cấp có thẩm quyền phê duyệt; và các nguồn kinh phí hợp pháp khác theo quy định của pháp luật.

2. Các khoản hỗ trợ tăng thêm hằng tháng, tiền công, thù lao, hỗ trợ và thu nhập đối với cá nhân thuộc chi thường xuyên, được bố trí trong dự toán chi thường xuyên hằng năm của cơ quan, đơn vị; không sử dụng vốn đầu tư công để chi trả các khoản này.

3. Các nhiệm vụ đầu tư hạ tầng kỹ thuật, hệ thống công nghệ, cơ sở dữ liệu, trang thiết bị, công cụ kỹ thuật chuyên dụng và các dự án đầu tư khác phục vụ bảo vệ an ninh mạng được bố trí từ nguồn vốn đầu tư theo quy định của pháp luật về đầu tư công và pháp luật có liên quan.

Điều 19. Tổ chức thực hiện

1. Bộ Công an chủ trì, phối hợp với Bộ Quốc phòng, bộ, ngành, địa phương tổ chức thực hiện Nghị định này; ban hành theo thẩm quyền hoặc trình cấp có thẩm quyền ban hành văn bản hướng dẫn các nội dung được giao trong Nghị định này.

2. Bộ Quốc phòng chủ trì thực hiện các nhiệm vụ thuộc phạm vi chức năng, nhiệm vụ, quyền hạn và hệ thống thông tin quân sự; phối hợp với Bộ Công an và các cơ quan liên quan trong tổ chức thực hiện Nghị định này.

Ban Cơ yếu Chính phủ giúp Bộ trưởng Bộ Quốc phòng tổ chức thực hiện Nghị định này trong phạm vi chức năng, nhiệm vụ, quyền hạn được giao.

3. Bộ Nội vụ, Bộ Tài chính, Bộ Khoa học và Công nghệ và các bộ, cơ quan có liên quan trong phạm vi chức năng, nhiệm vụ, quyền hạn của mình có trách nhiệm phối hợp, hướng dẫn và tổ chức thực hiện Nghị định này theo quy định của pháp luật.

4. Các bộ, ngành, địa phương, cơ quan, tổ chức, doanh nghiệp có trách nhiệm tổ chức thực hiện; xác định đầu mối phối hợp; xây dựng, rà soát, cập nhật quy chế nội bộ và bảo đảm điều kiện để thực hiện nhiệm vụ bảo vệ an ninh mạng theo quy định của pháp luật.

5. Cơ quan, đơn vị trực tiếp thực hiện chính sách, nhiệm vụ quy định tại Nghị định này chịu trách nhiệm về việc xác định đối tượng, điều kiện, mức hưởng, phạm vi nhiệm vụ, thời hạn, kết quả thực hiện; quản lý, sử dụng kinh phí đúng mục đích, đúng chế độ, hiệu quả và đúng quy định của pháp luật.

6. Tổ chức, cá nhân được tuyển chọn, tiếp nhận, bố trí, sử dụng, giao nhiệm vụ, đặt hàng, ký hợp đồng hoặc huy động tham gia bảo vệ an ninh mạng có trách nhiệm thực hiện đúng phạm vi, nội dung, thời hạn, yêu cầu chuyên môn, yêu cầu bảo mật và kết quả đầu ra đã được xác định; chịu trách nhiệm pháp lý đối với hành vi vi phạm và kết quả thực hiện nhiệm vụ theo quy định của pháp luật.

7. Việc thực hiện Nghị định này phải bảo đảm đúng đối tượng, đúng mục tiêu, đúng thẩm quyền, công khai, minh bạch trong phạm vi phù hợp với yêu cầu bảo vệ bí mật nhà nước, bí mật công tác; không làm phát sinh tổ chức, bộ máy, biên chế mới trái quy định; không chồng lặp, không hưởng trùng chế độ, chính sách có cùng tính chất, mục đích.

Điều 20. Hiệu lực thi hành

1. Nghị định này có hiệu lực thi hành từ ngày 19 tháng 8 năm 2026.

2. Kể từ ngày Nghị định này có hiệu lực thi hành, các quy định trước đây trái với Nghị định này hết hiệu lực thi hành.

Điều 21. Trách nhiệm thi hành

Bộ trưởng các Bộ: Công an, Quốc phòng, Tài chính, Nội vụ; Bộ trưởng, Thủ trưởng cơ quan ngang bộ, Chủ tịch Ủy ban nhân dân cấp tỉnh và cơ quan, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Nghị định này.

Nơi nhận:
- Ban Bí thư Trung ương Đảng;
- Thủ tướng, các Phó Thủ tướng Chính phủ;
- Các bộ, cơ quan ngang bộ;
- HĐND, UBND các tỉnh, thành phố trực thuộc trung ương;
- Văn phòng Trung ương và các Ban của Đảng;
- Văn phòng Tổng Bí thư;
- Văn phòng Chủ tịch nước;
- Hội đồng Dân tộc và các Ủy ban của Quốc hội;
- Văn phòng Quốc hội;
- Tòa án nhân dân tối cao;
- Viện kiểm sát nhân dân tối cao;
- Kiểm toán nhà nước;
- Ủy ban Trung ương Mặt trận Tổ quốc Việt Nam;
- Cơ quan trung ương của các tổ chức chính trị - xã hội;
- VPCP: BTCN, các PCN, Trợ lý TTg, các Vụ, Cục, Công báo;
- Lưu: VT, TCCV (2b). 14

TM. CHÍNH PHỦ
KT. THỦ TƯỚNG
PHÓ THỦ TƯỚNG

CHÍNH PHỦ NƯỚC CỘNG HÒA X.H.C.N VIỆT NAM

Phạm Gia Túc