ĐẢNG BỘ CHÍNH PHỦ
ĐẢNG ỦY
BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG
*
Số 12 -CTr/ĐU

ĐẢNG CỘNG SẢN VIỆT NAM

Hà Nội, ngày 27 tháng 3 năm 2026

CHƯƠNG TRÌNH HÀNH ĐỘNG
Thực hiện Chỉ thị số 57-CT/TW và Kế hoạch số 04-KH/BCĐTW về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu

---

Căn cứ Chỉ thị số 57-CT/TW ngày 31/12/2025 của Ban Bí thư về việc tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị;

Căn cứ Kế hoạch số 04-KH/BCĐTW ngày 05/01/2026 của Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị;

Căn cứ Nghị quyết Đại hội Đảng Bộ Nông nghiệp và Môi trường, nhiệm kỳ 2025 - 2030;

Thời gian qua, công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu đã được chú trọng trong quá trình chuyển đổi số, xây dựng cơ sở dữ liệu, phát triển Chính phủ số của Bộ. Tuy nhiên, công tác an toàn, an ninh thông tin chưa theo kịp thực tiễn; tình trạng một số hệ thống thông tin chưa đủ điều kiện an ninh mạng nhưng sử dụng vẫn tồn tại; hạ tầng chưa đồng bộ, ngân sách cho bảo đảm an toàn thông tin, an ninh mạng chưa đáp ứng yêu cầu. Dự báo tình hình an toàn, an ninh mạng có nhiều diễn biến phức tạp, trong bối cảnh dữ liệu trở thành tài nguyên chiến lược.

Nhằm tạo sự thống nhất về nhận thức, tư tưởng chính trị và hành động kiến tạo không gian mạng an toàn, tin cậy trong toàn Đảng bộ Bộ Nông nghiệp và Môi trường, Ban Thường vụ Đảng ủy Bộ ban hành Chương trình hành động thực hiện Chỉ thị số 57-CT/TW và Kế hoạch số 04-KH/BCĐTW về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu (sau đây viết tắt là Chương trình) với các nội dung trọng tâm như sau:

I. MỤC TIÊU VÀ YÊU CẦU

1. Mục tiêu chung

Xây dựng môi trường số, không gian mạng ngành nông nghiệp và môi trường an toàn, vững mạnh, có năng lực phòng vệ tốt và khả năng chống chịu

cao, bảo vệ vững chắc chủ quyền dữ liệu, lợi ích của ngành trên không gian mạng.

2. Mục tiêu cụ thể

a) Trọng tâm năm 2026

- Về lãnh đạo, chỉ đạo: Tạo chuyển biến mạnh mẽ về nhận thức và hành động trong toàn thể cán bộ, đảng viên, công chức, viên chức, người lao động thuộc Bộ. Rà soát, sửa đổi, hoàn thiện các quy định, các văn bản quản lý về bảo đảm an ninh mạng, an toàn thông tin dữ liệu.

- Về hạ tầng, dữ liệu: 100% hệ thống thông tin của cơ quan, đơn vị được rà soát, khắc phục lỗ hổng. Các hệ thống thông tin từ cấp độ 3 trở lên được ưu tiên bảo vệ, kết nối chia sẻ dữ liệu giám sát an ninh mạng 24/7 với Trung tâm An ninh mạng quốc gia (Bộ Công an). Hoàn thành kết nối mạng truyền số liệu chuyên dùng của Đảng và Nhà nước theo hướng thống nhất, dùng chung cho các cơ quan trong hệ thống chính trị để phục vụ việc trao đổi, xử lý văn bản mật tại Bộ.

- Về quản trị: Tăng cường kỷ luật, kỷ cương; thực hiện quản trị an ninh mạng dựa trên đánh giá rủi ro, tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật.

- Về Công nghệ, giải pháp: đẩy mạnh ứng dụng trí tuệ nhân tạo (AI) và các công nghệ tiên tiến để phát hiện sớm và xử lý kịp thời các mối đe doạ mạng.

b) Đến năm 2030

- Về văn bản quy phạm, quản lý, chỉ đạo: Hoàn thiện hệ thống các quy chế, quy định và hướng dẫn về an toàn thông tin mạng, an ninh mạng, bảo mật thông tin và an ninh dữ liệu; đảm bảo hành lang pháp lý đồng bộ, chặt chẽ theo quy định.

- Về quản trị: Triển khai tổ chức vận hành hạ tầng số và hệ thống thông tin theo hướng chủ động đưa Khung quản trị rủi ro an ninh mạng quốc gia vào thực tế để nhận diện, ngăn chặn và xử lý sớm các nguy cơ mất an toàn dữ liệu.

- Về Công nghệ, giải pháp: Đưa vào vận hành hiệu quả kiến trúc bảo vệ an ninh mạng đa lớp hiện đại, đồng bộ; triển khai ứng dụng các công nghệ tiên tiến, chuyển đổi sang phòng thủ chủ động, ứng dụng các giải pháp mã hoá hiện đại phục vụ bảo vệ dữ liệu quan trọng, dữ liệu bí mật thuộc phạm vi quản lý. Bảo đảm sử dụng sản phẩm, dịch vụ an ninh mạng "Make in Vietnam" chiếm tỉ trọng trên 50% trong các hệ thống của ngành.

- Về nhân lực: Tuyển dụng và xây dựng đội ngũ chuyên gia an ninh mạng trình độ cao, có năng lực thực chiến, đáp ứng yêu cầu của Bộ, ngành.

Định kỳ tổ chức đào tạo chuyên sâu cho đội ngũ chuyên trách chuyển đổi số; đồng thời phổ cập kiến thức, kỹ năng an toàn thông tin cơ bản cho toàn thể công chức, viên chức, người lao động các đơn vị trực thuộc Bộ.

c) Tầm nhìn đến năm 2045

Đáp ứng đầy đủ, bảo đảm an toàn thông tin mạng, an ninh mạng theo yêu cầu, chiến lược, kế hoạch thực hiện công tác an ninh mạng quốc gia.

3. Yêu cầu

- Quán triệt sâu sắc quan điểm bảo đảm an ninh mạng là nhiệm vụ trọng yếu, thường xuyên, cấp bách, đặt dưới sự lãnh đạo tuyệt đối của Đảng ủy Bộ. Chuyển dịch từ tư duy chiến lược "Phòng thủ bị động" sang "Phòng thủ tích cực, chủ động, toàn diện", xây dựng "Thế trận an ninh mạng chủ động, toàn diện"; xử lý từ sớm, từ xa mọi nguy cơ.

- Gắn trách nhiệm người đứng đầu với kết quả bảo đảm an ninh mạng, an ninh dữ liệu; coi đây là tiêu chí quan trọng trong đánh giá, quy hoạch, bổ nhiệm cán bộ lãnh đạo, quản lý các cấp.

- Chương trình hành động phải được triển khai đồng bộ, thống nhất trong toàn bộ các đơn vị trực thuộc Bộ; tuyệt đối tránh tình trạng thực hiện hình thức, dàn trải nguồn lực hoặc thiếu tập trung.

- Nâng cao quyết tâm chính trị trong thực thi nhiệm vụ, phải có sản phẩm cụ thể, kết quả đo lường được, bảo đảm tiến độ thực hiện đi đôi với hiệu quả thực chất.

II. NHIỆM VỤ TRỌNG TÂM NĂM 2026

1. Quán triệt sâu sắc quan điểm bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu là nhiệm vụ trọng yếu, thường xuyên, cấp bách; là trách nhiệm của cả hệ thống chính trị và toàn dân, đặt dưới sự lãnh đạo trực tiếp, toàn diện của Đảng, sự quản lý tập trung, thống nhất của Nhà nước.

2. Tổ chức quán triệt, tuyên truyền sâu rộng các nội dung của Chỉ thị 57-CT/TW và Kế hoạch 04-KH/BCĐTW và Chương trình hành động này tới 100% chi bộ, đơn vị trực thuộc.

3. Triển khai hoạt động Tiểu ban An toàn, An ninh mạng Bộ theo nhiệm vụ và theo sự phân công, chỉ đạo của Ban Chỉ đạo An ninh mạng quốc gia.

4. Rà soát, ban hành các quy định, tài liệu hướng dẫn về kiểm tra, đánh giá, bảo đảm an ninh mạng, an toàn thông tin mạng cho các cơ sở dữ liệu, hệ thống dùng chung; định kỳ tổ chức kiểm tra, đánh giá việc thực hiện các quy định đảm bảo an ninh mạng, an toàn thông tin theo quy định.

5. Rà soát, trình cấp có thẩm quyền xem xét tái cấu trúc, mở rộng, hiện

đại hóa và triển khai hoàn thiện hạ tầng số và an toàn thông tin mạng của Bộ theo hướng tập trung, chuẩn hoá trung tâm dữ liệu.

6. Rà soát, khắc phục tổng thể về an ninh mạng, bảo mật thông tin, an ninh dữ liệu đối với hệ thống thông tin của Bộ theo tiêu chuẩn TCVN 14423:2025 và nguồn nhân lực trong đó ưu tiên các hệ thống thông tin quan trọng, các CSDL quốc gia, chuyên ngành.

III. NHIỆM VỤ ĐẾN NĂM 2030

1. Nâng cao nhận thức

a) Tiếp tục quán triệt, nâng cao nhận thức về bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu, đặt dưới sự lãnh đạo trực tiếp, toàn diện của Đảng, sự quản lý tập trung, thống nhất của Nhà nước.

b) Đưa tiêu chí bảo đảm an toàn thông tin mạng, an ninh mạng vào đánh giá xếp loại thi đua, khen thưởng hằng năm của Bộ. Tham gia triển khai các giải pháp đánh giá tín nhiệm mạng, củng cố lòng tin, trách nhiệm của người dân khi hoạt động, tương tác, làm việc trên không gian mạng thuộc phạm vi quản lý.

c) Đổi mới mạnh mẽ công tác tuyên truyền, đưa nội dung bảo đảm an ninh mạng vào sinh hoạt chuyên đề, xây dựng "thế hệ công dân số". Nâng cao nhận thức, kiến thức, kỹ năng về an toàn thông tin mạng, an ninh mạng của cán bộ, đảng viên, công chức, viên chức người lao động thông qua phong trào "Bình dân học vụ số".

2. Xây dựng và hoàn thiện thể chế, quy định nội bộ

Rà soát, sửa đổi, bổ sung, hoàn thiện quy định về an toàn thông tin mạng, an ninh mạng, bảo mật thông tin thuộc phạm vi quản lý của Bộ. Triển khai áp dụng Khung quản trị rủi ro an ninh mạng đối với các hệ thống thông tin, cơ sở dữ liệu của Bộ; định kỳ đánh giá, phân loại rủi ro an ninh mạng và xây dựng phương án phòng ngừa, ứng phó phù hợp.

3. Phát triển hạ tầng an ninh mạng hiện đại, đồng bộ

a) Hiện đại hóa, chuẩn hóa, thông minh hóa hạ tầng số, an toàn thông tin mạng, an ninh mạng dùng chung đáp ứng yêu cầu công tác chuyển đổi số, triển khai kiến trúc bảo vệ an ninh mạng đa lớp bảo vệ tin cậy cho toàn bộ hạ tầng số, CSDL của Bộ; bảo đảm khả năng phòng vệ chủ động, phát hiện sớm, ngăn chặn và xử lý kịp thời các nguy cơ tấn công mạng. Quy hoạch và triển khai đồng bộ 5 nhóm giải pháp: (i) Bảo vệ hạ tầng mạng; (ii) Bảo vệ thiết bị đầu cuối; (iii) Bảo vệ ứng dụng, dịch vụ; (iv) Bảo vệ dữ liệu; (v) Bảo vệ người dùng, thực hiện "Phòng thủ chủ động", "Phòng thủ tích cực".

b) Bảo vệ tuyệt đối an toàn các CSDL quốc gia, lĩnh vực quan trọng, trọng yếu. Thiết lập cơ chế bảo mật "ngay từ thiết kế" đối với các trung tâm dữ liệu, hệ thống số, nền tảng số và ứng dụng mới; Kết nối, chia sẻ, đồng bộ dữ liệu liên thông giữa các đơn vị, với các bộ, ngành, địa phương trên nguyên tắc bảo mật, an toàn, đúng pháp luật, khắc phục tình trạng cát cứ, phân mảnh dữ liệu.

c) Tăng cường triển khai các giải pháp giám sát, cảnh báo sớm nguy cơ tấn công mạng; kết nối, chia sẻ dữ liệu giám sát, cảnh báo với Trung tâm An ninh mạng quốc gia và hệ thống giám sát an ninh mạng quốc gia theo quy định.

4. Bảo đảm nguồn lực tài chính, ngân sách

a) Thực hiện quy định an toàn thông tin mạng, an ninh mạng, an ninh dữ liệu là thành phần bắt buộc, ưu tiên trong mọi dự án công nghệ thông tin. Bảo đảm tỉ lệ kinh phí bình quân chi cho an toàn thông tin mạng, an ninh mạng đạt tối thiểu đạt 15% trong tổng kinh phí triển khai đề án, dự án, chương trình kế hoạch đầu tư công nghệ thông tin, chuyển đổi số.

b) Ưu tiên sử dụng các sản phẩm, dịch vụ an ninh mạng "Make in Vietnam", góp phần phát triển hệ sinh thái sản phẩm, giải pháp an ninh mạng trong nước và nâng cao năng lực tự chủ về công nghệ.

5. Bảo đảm nguồn nhân lực và hợp tác quốc tế

a) Tham gia các chương trình đào tạo chuyên sâu, huấn luyện thực chiến về kỹ năng giám sát, điều tra, ứng phó sự cố. Tổ chức, triển khai các khóa đào tạo, bồi dưỡng, nâng cao năng lực chuyên môn, kỹ năng giám sát, ứng phó sự cố, bảo vệ dữ liệu, an ninh mạng, an toàn thông tin.

b) Tham gia tích cực Mạng lưới liên kết các chuyên gia an ninh mạng trong nước và nước ngoài tham gia hỗ trợ công tác bảo đảm an ninh mạng.

c) Tăng cường hợp tác chia sẻ thông tin, cảnh báo sớm các nguy cơ tấn công mạng; tham gia các đợt diễn tập quốc tế do các cơ quan chuyên trách tổ chức

IV. TỔ CHỨC THỰC HIỆN

1. Phân công trách nhiệm

a) Các đồng chí Ủy viên Ban Thường vụ Đảng ủy Bộ, Ủy viên Ban chấp hành Đảng bộ Bộ theo lĩnh vực công tác được phân công, phụ trách chịu trách nhiệm toàn diện, lãnh đạo, chỉ đạo, kiểm tra và đôn đốc thực hiện công tác bảo đảm an toàn thông tin mạng, an ninh mạng, bảo mật thông tin.

b) Ủy ban Kiểm tra Đảng ủy Bộ chủ trì xây dựng kế hoạch và triển khai kiểm tra, giám sát các cấp ủy, tổ chức đảng, cơ quan, đơn vị trực thuộc Bộ thực hiện Kế hoạch này; định kỳ báo cáo Ban Thường vụ Đảng ủy Bộ.

c) Bí thư cấp uỷ, tổ chức đảng, cơ quan, đơn vị trực thuộc Bộ theo chức năng, nhiệm vụ được giao chịu trách nhiệm thực hiện các nhiệm vụ sau:

- Chịu trách nhiệm trực tiếp và toàn diện nếu để xảy ra sự cố an ninh mạng nghiêm trọng, đặc biệt là lộ, lọt bí mật nhà nước do yếu tố chủ quan, thiếu trách nhiệm hoặc không tuân thủ quy định.

- Trực tiếp tổ chức quán triệt, triển khai thực hiện Chương trình này đến đảng viên, công chức, viên chức, người lao động với các hình thức phù hợp, bám sát thực tiễn công tác của đơn vị.

- Triển khai thực hiện hiệu quả, thực chất, toàn diện nhiệm vụ, giải pháp tại Chỉ thị số 57-CT/TW, Kế hoạch số 04-KH/BCĐTW và các nhiệm vụ, giải pháp nêu tại Chương trình và Phụ lục kèm theo.

- Xây dựng kế hoạch thực hiện hoặc lồng ghép với các nhiệm vụ, đề án, chương trình cụ thể thuộc lĩnh vực quản lý nhà nước của đơn vị để tổ chức thực hiện bảo đảm đồng bộ, hiệu quả.

- Đưa kết quả đánh giá bảo đảm an toàn thông tin mạng, an ninh mạng của các cơ quan vào tiêu chí đánh giá tín nhiệm, năng lực của cán bộ, nhất là đối với người đứng đầu, để phục vụ công tác xếp loại hàng năm.

- Chủ động theo dõi, nắm chắc tình hình thực hiện chính sách pháp luật để kịp thời chỉ đạo xử lý hoặc kiến nghị cấp có thẩm quyền giải quyết các vấn đề phát sinh từ thực tiễn.

d) Vụ Tổ chức cán bộ chủ trì nghiên cứu, tham mưu đưa kết quả đánh giá bảo đảm an toàn thông tin mạng, an ninh mạng của các cơ quan, tổ chức vào tiêu chí đánh giá tín nhiệm, năng lực của cán bộ, nhất là đối với người đứng đầu, để phục vụ công tác xếp loại cán bộ, đảng viên hàng năm.

đ) Vụ Kế hoạch - Tài chính, Vụ Khoa học và Công nghệ chủ trì, tham mưu hướng dẫn, bố trí kinh phí ưu tiên nhiệm vụ, hạng mục về an toàn thông tin mạng, an ninh mạng; bảo đảm tỉ lệ kinh phí bình quân chi cho các sản phẩm, dịch vụ an ninh mạng, bảo mật thông tin, an ninh dữ liệu đạt tối thiểu 15% trong tổng kinh phí triển khai đề án, dự án, chương trình, kế hoạch đầu tư, ứng dụng, phát triển công nghệ thông tin, bảo đảm hiệu quả, đúng quy định, tránh lãng phí.

e) Cục Chuyển đổi số làm đầu mối, phối hợp với các cơ quan chuyên trách về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu; hướng

dẫn kỹ thuật việc triển khai các nhiệm vụ của Chương trình này.

2. Kinh phí thực hiện

a) Nguồn kinh phí thực hiện Chương trình được bảo đảm từ ngân sách nhà nước theo phân cấp, lồng ghép trong các chương trình, dự án đầu tư công, chuyển đổi số của ngành và các nguồn hợp pháp khác.

b) Ưu tiên bố trí ngân sách cho các nhiệm vụ cấp bách. Áp dụng linh hoạt các cơ chế tài chính đặc thù đã được phê duyệt nhằm đáp ứng yêu cầu tiến độ, bảo đảm thiết thực, hiệu quả, tránh lãng phí.

3. Chế độ thông tin, báo cáo

Cục Chuyển đổi số chủ trì, phối hợp với Văn phòng Đảng ủy Bộ, Vụ Khoa học và Công nghệ theo dõi, đôn đốc, kiểm tra thực hiện để tổng hợp thực hiện chế độ báo cáo định kỳ và báo cáo đột xuất theo yêu cầu và đề xuất với Ban Thường vụ Đảng ủy Bộ về các biện pháp cần thiết bảo đảm Chương trình được thực hiện đồng bộ, hiệu quả.

4. Sơ kết, tổng kết, đánh giá và khen thưởng, kỷ luật

a) Gắn kết quả thực hiện Chương trình với đánh giá, xếp loại mức độ hoàn thành nhiệm vụ của tập thể và cá nhân, đặc biệt là người đứng đầu.

b) Kịp thời biểu dương, khen thưởng các tập thể, cá nhân có thành tích xuất sắc, các mô hình hay, cách làm sáng tạo. Đồng thời, xem xét, xử lý nghiêm các trường hợp không hoàn thành nhiệm vụ, thiếu trách nhiệm, gây ảnh hưởng đến mục tiêu chung của Chương trình./.

T/M BAN THƯỜNG VỤ
BÍ THƯ

ĐẢNG CỘNG SẢN VIỆT NAM
ĐẢNG ỦY BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG
ĐẢNG BỘ CHÍNH PHỦ

Trần Đức Thắng

Nơi nhận:
- Ban Bí thư (để b/c),
- Thường trực Ban CĐTW về phát triển KHCN, ĐMST và CĐS (để b/c),
- Ban Thường vụ Đảng ủy Chính phủ (để b/c),
- Ban Chỉ đạo An ninh mạng QG (để b/c),
- Đ/c Bí thư Đảng ủy, Bộ trưởng,
- Các đ/c UVBCH Đảng bộ Bộ (để t/h),
- Các tổ chức đảng trực thuộc (để t/h),
- Các tổ chức đoàn thể của Bộ (để t/h),
- Các cơ quan tham mưu, giúp việc Đảng ủy Bộ,
- Lưu VPĐU, ĐUCĐS.

Phụ lục

DANH MỤC CÁC NHIỆM VỤ TRIỂN KHAI
CHƯƠNG TRÌNH HÀNH ĐỘNG CỦA ĐẢNG ỦY BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG

(Kèm theo Chương trình hành động số -CTr/ĐU ngày tháng 3 năm 2026 thực hiện Chỉ thị số 57-CT/TW và Kế hoạch số 04-KH/BCĐTW về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu của Đảng ủy Bộ Nông nghiệp và Môi trường)

TT	Tên nhiệm vụ	Cơ quan chủ trì	Cơ quan phối hợp	Kết quả	Thời gian hoàn thành
I	**HOÀN THIỆN THỂ CHẾ, CHỈ ĐẠO, TRIỂN KHAI**				
1.	Phối hợp, đề xuất sửa đổi, bổ sung các quy định pháp luật về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu và danh mục bảo vệ bí mật nhà nước để phù hợp với quy định mới tại Luật An ninh mạng, Luật Bảo vệ bí mật nhà nước.	Vụ Pháp chế	Cục CĐS; Văn phòng Bộ; Các đơn vị trực thuộc Bộ	Các văn bản quy phạm pháp luật được ban hành	Thường xuyên
2.	Rà soát, hoàn thiện, ban hành các quy định, văn bản quản lý, tài liệu hướng dẫn, đánh giá về bảo đảm an toàn thông tin dữ liệu, an ninh mạng	Cục CĐS	Các đơn vị trực thuộc Bộ	Các văn bản, nội dung quy phạm, quản lý được ban hành	Thường xuyên
3.	Tham mưu, triển khai các hoạt động của Tiểu ban An toàn, An ninh mạng Bộ Nông nghiệp và Môi trường theo sự phân công, chỉ đạo của Ban Chỉ đạo An ninh mạng quốc gia.	Cục CĐS	Các đơn vị trực thuộc Bộ	Hoạt động của Tiểu ban An toàn, An ninh mạng	Thường xuyên
4.	Xây dựng kế hoạch và thực hiện kiểm tra, giám sát thực hiện tại các cấp ủy, tổ chức đảng, cơ quan, đơn vị trực thuộc Bộ; định kỳ báo cáo theo yêu cầu của Ban Thường vụ Đảng ủy Bộ.	Ủy ban Kiểm tra Đảng ủy Bộ	Các đơn vị trực thuộc Bộ	Kế hoạch, kết quả kiểm tra, báo cáo	Thường xuyên
5.	Nghiên cứu, tham mưu đưa kết quả đánh giá bảo đảm an toàn thông tin mạng, an ninh mạng của các cơ quan, tổ chức vào tiêu	Vụ TCCB	Các đơn vị trực thuộc Bộ	Bổ sung quy chế, quy định của Đảng ủy Bộ,	Năm 2026

TT	Tên nhiệm vụ	Cơ quan chủ trì	Cơ quan phối hợp	Kết quả	Thời gian hoàn thành
	chí đánh giá tín nhiệm, năng lực của cán bộ, nhất là đối với người đứng đầu, để phục vụ công tác xếp loại cán bộ, đảng viên hàng năm.			Bộ Nông nghiệp và Môi trường	
II.	**HẠ TẦNG SỐ, CÔNG NGHỆ, GIẢI PHÁP**				
6.	Hoàn thành kết nối mạng truyền số liệu chuyên dùng của Đảng và Nhà nước theo hướng thống nhất, dùng chung cho các cơ quan trong hệ thống chính trị để phục vụ việc trao đổi, xử lý văn bản mật tại Bộ theo kế hoạch.	Cục CĐS	Các đơn vị trực thuộc Bộ	Hệ thống được triển khai theo hướng dẫn	Theo kế hoạch chung
7.	Tổ chức rà soát, đánh giá và củng cố Hệ thống giám sát an ninh mạng của Bộ, đảm bảo hoạt động giám sát và sẵn sàng ứng phó với các nguy cơ tấn công mạng, đồng thời có thể chia sẻ dữ liệu giám sát với hệ thống giám sát an ninh mạng quốc gia. Phối hợp với Bộ Công an và các cơ quan xây dựng phương án ứng cứu sự cố an ninh mạng cho hệ thống thuộc phạm vi quản lý.	Cục CĐS	Các đơn vị trực thuộc Bộ	Hệ thống giám sát mạng của Bộ; phương án ứng cứu sự cố	Tháng 5/2026
8.	Triển khai các giải pháp kỹ thuật nhằm bảo đảm an toàn thông tin mạng, an ninh mạng cho các hệ thống thông tin và cơ sở dữ liệu thuộc phạm vi quản lý của Bộ; ưu tiên khắc phục các lỗ hổng bảo mật và tăng cường bảo vệ các hệ thống thông tin quan trọng.	Các đơn vị trực thuộc Bộ	Cục CĐS	Các giải pháp được triển khai	Tháng 4/2026
9.	Phối hợp với các cơ quan liên quan để tổ chức trình thẩm định, phê duyệt cấp độ an toàn thông tin đúng quy định với toàn bộ các hệ thống thông tin, hạ tầng đang sử dụng, trực tiếp quản lý.	Các đơn vị trực thuộc Bộ quản lý vận hành các hệ thống thông tin, cơ sở dữ liệu	Cục CĐS	Quyết định Phê duyệt cấp độ và phương án bảo đảm an toàn thông tin theo cấp độ	Tháng 4/2026

TT	Tên nhiệm vụ	Cơ quan chủ trì	Cơ quan phối hợp	Kết quả	Thời gian hoàn thành
10.	Bảo đảm tất cả các hệ thống thông tin mới xây dựng hoặc nâng cấp phải thực hiện phê duyệt cấp độ an toàn thông tin và triển khai phương án bảo đảm an toàn thông tin trước khi đưa vào vận hành chính thức.	Các đơn vị trực thuộc Bộ	Cục CĐS	Quyết định Phê duyệt cấp độ và phương án bảo đảm an toàn thông tin theo cấp độ	Thường xuyên
11.	Rà soát, đánh giá tổng thể về an toàn thông tin mạng, an ninh mạng và an ninh dữ liệu đối với các cơ sở dữ liệu quốc gia, chuyên ngành, các hệ thống thông tin và nguồn nhân lực (phối hợp với các đơn vị thuộc Bộ Công an, Ban Cơ yếu Chính phủ). Xác định các nguy cơ, điểm yếu về bảo mật và kiến nghị, đề xuất giải pháp khắc phục.	Các đơn vị trực thuộc Bộ quản lý vận hành các hệ thống thông tin, cơ sở dữ liệu	Cục CĐS	Kết quả rà soát, đánh giá. Kiến nghị, đề xuất giải pháp khắc phục	Tháng 6/2026
12.	Phối hợp với Bộ Công an thiết lập kênh kết nối, trao đổi thông tin, chia sẻ dữ liệu giám sát/cảnh báo với hệ thống giám sát an ninh mạng quốc gia, Trung tâm An ninh mạng quốc gia theo hướng dẫn; ưu tiên các hệ thống từ cấp độ 3 trở lên do Bộ quản lý.	Cục CĐS	Các đơn vị trực thuộc Bộ	Đáp ứng các yêu cầu kỹ thuật theo hướng dẫn	Tháng 5/2026
13.	Thực hiện báo cáo về sự cố trong vòng 24h nếu xảy ra và tuân theo sự điều phối ứng phó sự cố của lực lượng chuyên trách bảo vệ an ninh mạng Bộ Công an theo quy định.	Cục CĐS	Các đơn vị trực thuộc Bộ	Báo cáo	Thường xuyên
14.	Triển khai mô hình bảo đảm an toàn thông tin "4 lớp" đối với hạ tầng số và các hệ thống thông tin của Bộ, bao gồm: lực lượng tại chỗ; hệ thống giám sát an ninh mạng; đơn vị kiểm tra, đánh giá độc lập; và kết nối với hệ thống giám sát an ninh mạng quốc gia.	Cục CĐS	Các đơn vị trực thuộc Bộ quản lý vận hành các hệ thống thông tin, cơ sở dữ liệu	Đáp ứng các yêu cầu kỹ thuật theo hướng dẫn	Tháng 4/2026

TT	Tên nhiệm vụ	Cơ quan chủ trì	Cơ quan phối hợp	Kết quả	Thời gian hoàn thành
15.	Tổ chức kiểm tra, đánh giá định kỳ việc thực hiện các quy định đảm bảo an toàn thông tin mạng, an ninh mạng theo quy định; mức độ bảo đảm an ninh mạng đối với các đơn vị trực thuộc Bộ theo bộ chỉ số đánh giá an ninh mạng quốc gia; kết quả đánh giá được sử dụng làm căn cứ phục vụ công tác quản lý, điều hành và đánh giá mức độ hoàn thành nhiệm vụ của các cơ quan, đơn vị.	Cục CĐS	Các đơn vị trực thuộc Bộ	Báo cáo kiểm tra, đánh giá	Thường xuyên
16.	Tổ chức, tham gia các khóa đào tạo, bồi dưỡng, nâng cao năng lực chuyên môn, kỹ năng giám sát, ứng phó sự cố, bảo vệ dữ liệu, an ninh mạng, an toàn thông tin mạng.	Cục CĐS	Các đơn vị trực thuộc Bộ	Đáp ứng yêu cầu theo hướng dẫn	Thường xuyên
17.	Tổ chức diễn tập ứng cứu sự cố an ninh mạng định kỳ đối với các hệ thống thông tin quan trọng; nâng cao năng lực phát hiện, ứng phó và khắc phục sự cố an ninh mạng trong phạm vi quản lý của Bộ.	Cục CĐS	Các đơn vị trực thuộc Bộ	Các cuộc diễn tập định kỳ hàng năm	Định kỳ hằng năm
18.	Tăng cường công tác thông tin, tuyên truyền, truyền thông về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu ngành nông nghiệp và môi trường	Báo Nông nghiệp và Môi trường	Tạp chí Nông nghiệp và Môi trường; Cổng Thông tin điện tử (Văn phòng Bộ); các đơn trực thuộc Bộ	Các chương trình, sản phẩm thông tin, tuyên truyền, truyền thông về đảm bảo an ninh mạng, bảo mật thông tin và an ninh dữ liệu	Thường xuyên