UBND TỈNH PHÚ THỌ **SỞ NÔNG NGHIỆP VÀ MÔI TRƯỜNG**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 1230 /QĐ-SNNMT	*Phú Thọ, ngày 23 tháng 9 năm 2025*

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn thông tin mạng trong việc ứng dụng công nghệ thông tin, chuyển đổi số của Sở Nông nghiệp và Môi trường tỉnh Phú Thọ

GIÁM ĐỐC SỞ NÔNG NGHIỆP VÀ MÔI TRƯỜNG

Căn cứ Luật Công nghệ thông tin năm 2006;

Căn cứ Luật An toàn thông tin mạng năm 2015;

Căn cứ Luật An ninh mạng năm 2018;

Căn cứ Luật Bảo vệ bí mật nhà nước năm 2018;

Căn cứ Luật giao dịch điện tử 2023 và Nghị định 59/2022/NĐ-CP ngày 05 tháng 9 năm 2022 của Chỉnh phủ;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 53/2022/NĐ-CP ngày 15 tháng 8 năm 2022 của Chính phủ về quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Nghị định số 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 của Chính phủ về bảo vệ dữ liệu cá nhân;

Căn cứ Nghị định số 147/2024/NĐ-CP ngày 09 tháng 11 năm 2024 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng;

Căn cứ Nghị định số 35/2025/NĐ-CP ngày 25 tháng 02 năm 2025 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Nông nghiệp và Môi trường;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Căn cứ Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị

định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Tiêu chuẩn Việt Nam TCVN 11930:2017 Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 09/2025/QĐ-UBND ngày 01 tháng 7 năm 2025 của Ủy ban nhân dân tỉnh Phú Thọ ban hành Quy định vị trí, chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Nông nghiệp và Môi trường tỉnh Phú Thọ;

Theo đề nghị của Chánh Văn phòng Sở Nông nghiệp và Môi trường.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin mạng trong việc ứng dụng công nghệ thông tin, chuyển đổi số của Sở Nông nghiệp và Môi trường tỉnh Phú Thọ *(Có Quy chế bảo đảm an toàn thông tin mạng trong việc ứng dụng công nghệ thông tin, chuyển đổi số kèm theo).*

Điều 2. Quyết định này có hiệu lực kể từ ngày ký.

Điều 3. Chánh Văn phòng Sở, Trưởng các phòng chuyên môn, Thủ trưởng các đơn vị trực thuộc Sở, công chức, viên chức, người lao động Sở Nông nghiệp và Môi trường tỉnh Phú Thọ và các cơ quan, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Công an tỉnh;
- Sở KHCN;
- GĐ, các PGĐ Sở;
- Lưu: VT, VP.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ NÔNG NGHIỆP VÀ MÔI TRƯỜNG
TỈNH PHÚ THỌ

Nguyễn Huy Nhuận

UBND TỈNH PHÚ THỌ
SỞ NÔNG NGHIỆP VÀ MÔI TRƯỜNG

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

QUY CHẾ
Bảo đảm an toàn thông tin mạng trong việc ứng dụng công nghệ thông tin, chuyển đổi số của Sở Nông nghiệp và Môi trường tỉnh Phú Thọ

(Ban hành kèm theo Quyết định số 1230 */QĐ-SNNMT ngày 23 tháng 9 năm 2025 của Giám đốc Sở Nông nghiệp và Môi trường tỉnh Phú Thọ)*

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của Sở Nông nghiệp và Môi trường, các phòng thuộc sở; cơ quan, đơn vị trực thuộc (sau đây gọi là các cơ quan, đơn vị).

Điều 2. Đối tượng áp dụng

Quy chế này được áp dụng đối với Sở Nông nghiệp và Môi trường tỉnh Phú Thọ, các cơ quan, đơn vị trực thuộc và các tổ chức, cá nhân khi đến làm việc có kết nối với hệ thống mạng LAN nội bộ, mạng máy tính và kết nối các phần mềm dùng chung, Cổng thông tin điện tử của Sở Nông nghiệp và Môi trường.

Điều 3. Giải thích từ ngữ

Trong Quy chế này, các từ ngữ dưới đây được hiểu như sau:

1. *An toàn thông tin mạng* là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

2. *An ninh mạng* là việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

3. *Hệ thống thông tin* là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng.

4. *Hạ tầng kỹ thuật* là tập hợp các thiết bị tính toán, lưu trữ, thiết bị ngoại vi, thiết bị kết nối mạng, thiết bị phụ trợ, đường truyền, mạng nội bộ, mạng diện rộng…

5. *Chủ quản hệ thống thông tin* là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin.

6. *Cổng thông tin điện tử* là điểm truy cập duy nhất của cơ quan, đơn vị trên môi trường mạng, liên kết, tích hợp các kênh thông tin, các dịch vụ và các ứng dụng mà qua đó người dùng có thể khai thác, sử dụng và cá nhân hóa việc hiển thị thông tin.

7. *Sự cố an toàn thông tin mạng* là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

8. *Mạng* là một hệ thống kết nối nhiều thiết bị với nhau (như máy tính, điện thoại, máy in, máy chủ…) nhằm mục đích chia sẻ dữ liệu, tài nguyên và thông tin.

9. *Người dùng* là cán bộ, công chức, viên chức, người lao động tại các cơ quan, đơn vị thuộc Sở sử dụng thiết bị số để xử lý công việc.

10. *Phần mềm độc hại* là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

11. *Thiết bị số* là thiết bị điện tử, máy tính, viễn thông, truyền dẫn, thu phát sóng vô tuyến điện và thiết bị tích hợp khác được sử dụng để sản xuất, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin số.

12. *Mật khẩu mạnh* là mật khẩu có độ dài tối thiểu 10 ký tự, trong đó kết hợp bao gồm ký tự hoa, thường, chữ số và ký tự đặc biệt.

Điều 4. Nguyên tắc bảo đảm an toàn thông tin mạng

1. Bảo đảm an toàn thông tin mạng, an ninh mạng là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt quá trình liên quan đến thông tin và thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ hệ thống thông tin. Bảo đảm an toàn, an ninh thông tin tuân thủ các nguyên tắc chung quy định tại Điều 4 Luật An toàn thông tin mạng và Điều 4 Nghị định số 85/2016/NĐ-CP và các quy định pháp luật khác có liên quan.

2. Tuân thủ các quy định và hướng dẫn về bảo đảm an toàn thông tin mạng, an ninh mạng của cơ quan có thẩm quyền. Trường hợp có văn bản, quy định cập nhật, thay thế hoặc quy định khác tại văn bản quy phạm pháp luật, quyết định của cấp có thẩm quyền cao hơn thì áp dụng quy định tại văn bản đó.

3. Trách nhiệm bảo đảm an toàn thông tin mạng và an ninh mạng gắn với trách nhiệm của người đứng đầu cơ quan, đơn vị và cá nhân trực tiếp liên quan.

4. Việc bảo đảm an toàn hệ thống thông tin được thực hiện một cách tổng thể, đồng bộ, tập trung trong việc đầu tư các giải pháp bảo vệ, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp. Các nhiệm vụ, dự án ứng dụng công nghệ thông tin hoặc có cấu phần công nghệ thông tin quy định tại khoản 1 và khoản 2 Điều 1 của Nghị định số 73/2019/NĐ-CP và khoản 1, Điều 1 của Nghị định số 82/2024/NĐ-CP phải có ý kiến thẩm định nội dung liên quan đến an toàn, an ninh thông tin, phê duyệt hồ sơ cấp độ và phương án bảo đảm an toàn hệ thống thông tin theo cấp độ trước khi được phê duyệt.

5. Quản lý, sử dụng và bảo đảm an ninh mạng, mạng máy tính nội bộ có lưu trữ, truyền đưa bí mật nhà nước phải được tách biệt vật lý hoàn toàn với mạng máy tính, các thiết bị, phương tiện điện tử có kết nối mạng Internet, trường hợp khác phải bảo đảm quy định của pháp luật về bảo vệ bí mật nhà nước.

6. Xử lý sự cố an toàn thông tin phải phù hợp với trách nhiệm, quyền hạn và bảo đảm lợi ích hợp pháp của cơ quan, đơn vị, cá nhân liên quan và theo quy định của pháp luật.

7. Mỗi công chức, viên chức, người lao động tại các đơn vị thuộc Sở nêu cao tinh thần chủ động, tự giác trong việc áp dụng các biện pháp bảo đảm an toàn, an ninh mạng.

Điều 5. Các hành vi bị cấm

1. Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật An toàn thông tin mạng, Điều 8 Luật An ninh mạng và Điều 5 Luật Bảo vệ bí mật nhà nước.

2. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập mạng không dây của cá nhân vào mạng nội bộ; tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin cài đặt trên thiết bị công nghệ thông tin phục vụ công việc; tự ý thay thế, lắp mới, tráo đổi thành phần của máy tính phục vụ công việc.

3. Tiết lộ thiết kế, thông số cấu hình hệ thống cho tổ chức, cá nhân khác khi không được phép; tìm cách truy cập dưới bất cứ hình thức nào vào các khu vực không được phép truy cập.

4. Sử dụng hạ tầng, trang thiết bị công nghệ thông tin của cơ quan, đơn vị để đào tiền ảo, đánh bạc, cá độ.

5. Phát tán thư rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.

6. Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân.

7. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

8. Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới khả năng truy cập hệ thống thông tin của người sử dụng.

9. Các hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

Chương II

AN TOÀN THÔNG TIN MẠNG TRONG THIẾT KẾ, XÂY DỰNG, VẬN HÀNH HỆ THỐNG THÔNG TIN

Điều 6. An toàn thông tin mạng trong thiết kế, xây dựng, vận hành hệ thống thông tin

1. Các hoạt động liên quan đến xây dựng, thiết lập, quản lý, vận hành, nâng cấp mở rộng hệ thống thông tin phải thực hiện xác định cấp độ và phương án bảo đảm an toàn thông tin mạng theo quy định tại Nghị định số 85/2016/NĐ-CP và Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Thiết kế, xây dựng, đầu tư các giải pháp bảo đảm an toàn thông tin phải tuân thủ nguyên tắc đồng bộ, có thể dùng chung, chia sẻ để tối ưu hiệu năng thiết bị và hiệu quả đầu tư.

3. Trước khi đưa vào vận hành, khai thác hệ thống thông tin, đơn vị được giao chủ đầu tư phải phối hợp với tổ chức chuyên môn có đủ năng lực, được cơ quan có thẩm quyền cấp phép thực hiện đánh giá, kiểm định an toàn thông tin mạng. Tổ chức hiệu chỉnh theo kết quả đánh giá, kiểm định để hạn chế, phòng ngừa rủi ro, nguy cơ xảy ra mất an toàn thông tin mạng.

Điều 7. An toàn thông tin mạng đối với thuê dịch vụ công nghệ thông tin

1. Khi ký kết hợp đồng thuê dịch vụ công nghệ thông tin, cơ quan chủ trì thuê dịch vụ phải xác định rõ phạm vi, trách nhiệm, quyền hạn và nghĩa vụ của các bên về bảo đảm an toàn thông tin mạng, điều kiện xử lý vi phạm quy định bảo đảm an toàn thông tin mạng và trách nhiệm bồi thường thiệt hại do hành vi vi phạm của bên cung cấp dịch vụ gây ra.

2. Trong quá trình sử dụng dịch vụ công nghệ thông tin, cơ quan chủ trì thuê dịch vụ có trách nhiệm:

a) Yêu cầu bên cung cấp dịch vụ phải bảo mật thông tin, dữ liệu, mã nguồn, tài liệu thiết kế hệ thống thông tin; triển khai các biện pháp bảo đảm an toàn thông tin mạng tuân thủ phương án bảo đảm an toàn thông tin được cấp có thẩm quyền phê duyệt, các quy định tại Quy chế này, Luật An toàn thông tin mạng và các quy định khác của pháp luật có liên quan;

b) Quản lý thông tin, dữ liệu phát sinh từ dịch vụ đã thuê; bảo đảm bên cung cấp dịch vụ không được truy cập để quản trị dữ liệu thuộc phạm vi nhà nước quản lý lưu trữ trên hệ thống thuê;

c) Giám sát, giới hạn quyền của bên cung cấp dịch vụ khi cho phép truy cập vào hệ thống thông tin để xử lý sự cố hoặc hỗ trợ câng cấp, quản trị, vận hành.

3. Khi phát hiện bên cung cấp dịch vụ có dấu hiệu vi phạm quy định bảo đảm an toàn thông tin mạng, cơ quan chủ trì thuê dịch vụ có trách nhiệm:

a) Tạm dừng hoặc đình chỉ hoạt động của hệ thống thông tin tùy theo mức độ vi phạm và thông báo cho bên cung cấp dịch vụ;

b) Thu hồi quyền truy cập hệ thống thông tin đã cấp cho bên cung cấp dịch vụ (nếu có);

c) Kiểm tra, xác định, mức độ vi phạm và thiệt hại xảy ra; thông báo cho bên cung cấp dịch vụ; tiến hành các thủ tục xử lý vi phạm và bồi thường thiệt hại hoặc xử lý theo các quy định của pháp luật.

4. Kết thúc thời gian thuê dịch vụ, cơ quan chủ trì thuê dịch vụ có trách nhiệm:

a) Yêu cầu bên cung cấp dịch vụ chuyển giao đầy đủ thông tin, dữ liệu và các công cụ cần thiết để bảo đảm có thể khai thác sử dụng được thông tin, dữ liệu kể cả trong trường hợp thay đổi bên cung cấp dịch vụ.

b) Thu hồi và thay đổi mật khẩu hoặc hủy bỏ tài khoản truy cập hệ thống thông tin đã cấp cho bên cung cấp dịch vụ.

Điều 8. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

Hệ thống thông tin khi kết thúc vận hành, khai thác hoặc thanh lý, hủy bỏ phải tuân thủ các quy định của pháp luật về quản lý tài sản. Thông tin, dữ liệu trên các hệ thống thông tin phải được sao lưu và chuyển sang các hệ thống khác (nếu còn giá trị sử dụng). Thực hiện các biện pháp xóa, hủy dữ liệu trước khi thanh lý, hủy tài sản.

Điều 9. Giám sát an toàn hệ thống thông tin mạng, an ninh mạng

Đối với các hệ thống thông tin được lưu ký tại các trung tâm dữ liệu của các doanh nghiệp hoặc sử dụng máy chủ riêng đặt tại trụ sở, cơ quan chủ đầu tư hệ thống thông tin có trách nhiệm tự tổ chức giám sát an toàn hệ thống thông tin mạng, an ninh mạng.

Điều 10. Kiểm tra, đánh giá an toàn thông tin mạng

1. Trong quá trình vận hành hệ thống thông tin, các cơ quan, đơn vị vận hành hệ thống thông tin có trách nhiệm tổ chức kiểm tra, đánh giá an toàn thông tin mạng đối với hệ thống thông tin do cơ quan mình quản lý.

2. Nội dung, tần suất kiểm tra đánh giá thực hiện theo Điều 11, Điều 12 Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

3. Việc kiểm tra, đánh giá an toàn thông tin mạng phải do tổ chức chuyên môn được cơ quan có thẩm quyền cấp phép; tổ chức sự nghiệp nhà nước có chức

năng, nhiệm vụ phù hợp hoặc do tổ chức chuyên môn được cấp có thẩm quyền chỉ định thực hiện.

Điều 11. Xử lý rủi ro an toàn thông tin

Trên cơ sở báo cáo kết quả kiểm tra, đánh giá an toàn thông tin mạng hoặc cảnh báo nguy cơ gây mất an toàn thông tin mạng từ Công an tỉnh, Sở Khoa học và Công nghệ hoặc các cơ quan có thẩm quyền khác, đơn vị vận hành hệ thống thông tin có trách nhiệm tự khắc phục hoặc lựa chọn đơn vị đủ năng lực để triển khai các phương án khắc phục. Kết thúc xử lý, báo cáo kết quả thực hiện về Công an tỉnh, Sở Khoa học và Công nghệ để theo dõi, tổng hợp.

Điều 12. Ứng cứu xử lý sự cố an toàn thông tin mạng

1. Nguyên tắc ứng cứu xử lý sự cố

a) Chủ động, kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả.

b) Phối hợp chặt chẽ, tuân thủ quy định của pháp luật về điều phối ứng cứu sự cố an toàn thông tin mạng.

c) Ưu tiên ứng cứu, xử lý sự cố bằng lực lượng tại chỗ và trách nhiệm chính của Đơn vị vận hành hệ thống thông tin.

d) Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của cơ quan, cá nhân; bảo mật thông tin cá nhân, thông tin riêng của cơ quan khi tham gia các hoạt động ứng cứu xử lý sự cố.

2. Phân loại sự cố an toàn thông tin mạng

a) Sự cố do bị tấn công mạng: tấn công từ chối dịch vụ; tấn công giả mạo; tấn công sử dụng mã độc; tấn công truy cập trái phép, chiếm quyền điều khiển; tấn công thay đổi giao diện; tấn công mã hóa phần mềm, dữ liệu, thiết bị; tấn công phá hoại thông tin, dữ liệu, phần mềm; tấn công nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu; các hình thức tấn công khác.

b) Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật.

c) Sự cố do lỗi của cán bộ quản trị, vận hành hệ thống.

d) Sự cố do các thảm họa tự nhiên.

3. Phân loại mức độ sự cố

a) Thấp: Sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan.

b) Trung bình: Sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của cơ quan.

c) Cao: Sự cố tác động đến khả năng vận hành của hệ thống thông tin, ảnh hưởng đến dữ liệu, thiết bị, gây ảnh hưởng đến hoạt động chung của cơ quan và hoạt động cung cấp dịch vụ công cho người dân, doanh nghiệp.

d) Nghiêm trọng: Sự cố gây gián đoạn hoặc đình trệ hệ thống trong một khoảng thời gian ngắn, ảnh hưởng nghiêm trọng đến dữ liệu, thiết bị của hệ thống, gây thiệt hại nghiêm trọng cho cơ quan, người dân, doanh nghiệp.

đ) Đặc biệt nghiêm trọng: Sự cố làm tê liệt toàn bộ hoạt động của hệ thống, gây thiệt hại đặc biệt nghiêm trọng cho cơ quan, người dân, doanh nghiệp, đe dọa trật tự an toàn xã hội.

2. Quy trình ứng cứu sự cố thực hiện theo Điều 11 Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc. Báo cáo ban đầu sự cố và Báo cáo hoàn thành xử lý sự cố khi thực hiện quy trình ứng cứu sự cố được thực hiện theo Mẫu số 01 và Mẫu số 02 tại Phụ lục kèm theo Quy chế này.

3. Trường hợp có sự cố nghiêm trọng ở mức độ cao trở lên hoặc vượt quá khả năng khắc phục của đơn vị, lãnh đạo đơn vị phải báo cáo khẩn cấp cho cơ quan cấp trên quản lý trực tiếp và Công an tỉnh, Sở Khoa học và Công nghệ để được hướng dẫn, hỗ trợ hoặc điều phối ứng cứu sự cố an toàn thông tin mạng.

4. Quá trình xử lý sự cố phải được ghi chép và lưu trữ tại đơn vị; bảo toàn bằng chứng, chứng cứ phục vụ cho việc kiểm tra, xử lý, khắc phục và phòng ngừa sự cố. Trong trường hợp sự cố có liên quan đến các vi phạm pháp luật, đơn vị có trách nhiệm thu thập và cung cấp chứng cứ cho cơ quan có thẩm quyền theo quy định của pháp luật.

Chương III
BIỆN PHÁP BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 13. Bảo đảm an toàn vật lý và môi trường

1. Các khu vực xử lý, lưu trữ thông tin, phương tiện xử lý thông tin, phương tiện bảo đảm an toàn thông tin mạng phải được đặt ở vị trí an toàn, bảo vệ bằng tường bao và kiểm soát ra vào, bảo đảm chỉ có người có nhiệm vụ mới được vào và phải có nội quy riêng khi làm việc trong các khu vực này.

2. Các khu vực tại Khoản 1 Điều này phải có biện pháp bảo vệ phòng chống cháy nổ, ngập lụt, chống sét, tác động của môi trường và các thảm họa khác do thiên nhiên và con người gây ra.

3. Bảo đảm thiết bị lưu trữ dữ liệu quan trọng, phần mềm bản quyền lưu trữ trên thiết bị phải được kiểm tra, xóa hoặc ghi đè không có khả năng khôi phục trước khi loại bỏ hoặc tái sử dụng cho mục đích khác.

Điều 14. Quản lý an toàn hạ tầng mạng

1. An toàn cho mạng nội bộ

a) Đối với các mạng LAN sử dụng mạng chuyên dùng của tỉnh phải sử dụng thiết bị tường lửa chuyên dụng hoặc phần mềm tường lửa để ngăn chặn và phát hiện xâm nhập trái phép vào mạng nội bộ của cơ quan khi kết nối với hệ thống bên ngoài; đối với các mạng LAN chưa sử dụng chuyên dùng khuyến khích sử dụng thiết bị tường lửa chuyên dụng hoặc phần mềm tường lửa để ngăn chặn và phát hiện xâm nhập trái phép vào mạng nội bộ của cơ quan khi kết nối với hệ thống bên ngoài.

b) Khi kết nối từ xa vào mạng nội bộ, phải sử dụng giao thức mạng có mã hóa thông tin và thiết lập mật khẩu mạnh.

2. Mạng không dây để kết nối với mạng nội bộ phải thiết lập mật khẩu mạnh, mã hóa dữ liệu theo cơ chế bảo mật WPA2 hoặc WPA3. Mật khẩu truy cập phải được thay đổi định kỳ 06 tháng/lần.

3. Hệ điều hành, phần mềm tích hợp trên các thiết bị mạng phải thường xuyên được cập nhật các bản vá lỗi theo khuyến nghị của các nhà sản xuất.

4. Phải lưu trữ nhật ký khi thay đổi cấu hình kỹ thuật của các thiết bị mạng.

Điều 15. Quản lý an toàn máy chủ và ứng dụng

1. Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ

a) Máy chủ phải được cài đặt, sử dụng phần mềm phòng chống mã độc Phần mềm phòng chống mã độc được cập nhật thường xuyên và phải có tính năng kỹ thuật đáp ứng yêu cầu của Bộ Khoa học và Công nghệ.

b) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn.

c) Thiết lập chế độ tự động cập nhật bản vá hệ điều hành, phần mềm, ứng dụng và hệ quản trị cơ sở dữ liệu được cài đặt trên máy chủ, phải thiết lập mật khẩu truy nhập chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng đối với tất cả máy chủ.

d) Thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng.

đ) Thường xuyên kiểm tra cấu hình, các tệp tin nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện và xử lý những sự cố nếu có.

e) Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp.

g) Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng.

h) Bảo đảm các kết nối mạng trên máy chủ hoạt động liên tục, ổn định và an toàn. Cấu hình, kiểm soát các kết nối, các cổng dịch vụ từ bên trong đi ra, bên ngoài đi vào hệ thống.

i) Tất cả máy chủ, thiết bị công nghệ thông tin không được kết nối với Internet trừ trường hợp bắt buộc.

2. Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống trước khi đưa vào vận hành, khai thác.

a) Xây dựng, áp dụng quy trình cấu hình tối ưu, tăng cường bảo mật cho các máy chủ.

b) Máy chủ phải được rà soát, cấu hình tối ưu, tăng cường bảo mật trước khi đưa hệ thống vào vận hành khai thác.

3. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố.

a) Triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

b) Phải thực hiện lưu trữ thay đổi cấu hình kỹ thuật của máy chủ, hệ điều hành, phần mềm.

4. Nghiêm cấm sử dụng các tài nguyên tính toán, gồm: các máy chủ và các cổng dịch vụ môi trường mạng để xây dựng các hệ thống thực hiện các hành vi đào tiền ảo, rà quét các lỗ hổng bảo mật, hoặc tham gia các hoạt động bất hợp pháp khác trên môi trường mạng.

Điều 16. Bảo đảm an toàn dữ liệu

1. Quản lý tài khoản truy cập

a) Khi cấp tài khoản lần đầu cho người dùng, đơn vị vận hành hệ thống thông tin phải thông báo cho người dùng. Người dùng có trách nhiệm thay đổi mật khẩu sau khi đăng nhập thành công lần đầu. Chậm nhất là 03 ngày, các tài khoản không tuân thủ việc thay đổi mật khẩu phải được tự động vô hiệu hóa.

b) Các hệ thống thông tin phải thiết lập giới hạn số lần đăng nhập không hợp lệ tối đa không quá 05 lần; tự động kết thúc phiên làm việc nếu quá 30 phút người dùng không tương tác với hệ thống.

c) Khi cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc, nghỉ hưu, đơn vị quản lý cá nhân đó phải thông báo cho đơn vị vận hành hệ thống thông tin để điều chỉnh, thu hồi hoặc hủy bỏ tài khoản.

d) Không thiết lập cùng một mật khẩu cho nhiều tài khoản quản trị của hệ thống thông tin.

đ) Tài khoản quản trị, tài khoản người dùng phải được rà soát hàng năm, đảm bảo các tài khoản và quyền truy cập hệ thống được cấp phát đúng. Các tài khoản không sử dụng trong thời gian 01 năm phải bị khóa hoặc xóa bỏ.

e) Không sử dụng tài khoản thư điện tử công vụ (***@phutho.gov.vn) để giao dịch, đăng ký trên mạng xã hội và hệ thống thông tin công cộng.

2. Tên miền (***.phutho.gov.vn) khi không còn sử dụng, các cơ quan phải có văn bản đề nghị thu hồi tên miền.

3. Các hệ thống thông tin lưu ký tại các nhà cung cấp dịch vụ khi không còn sử dụng, phải thực hiện lưu trữ dữ liệu ra thiết bị lưu trữ ngoài và yêu cầu đơn vị cung cấp dịch vụ lưu ký xóa hoàn toàn dữ liệu trên các máy chủ.

4. Khi chia sẻ tài nguyên trên máy chủ hoặc máy trạm phải sử dụng mật khẩu để bảo vệ thông tin, dữ liệu; không thiết lập chế độ chia sẻ toàn bộ ổ cứng; kết thúc chia sẻ tài nguyên khi hoàn thành.

5. Khi bảo hành, bảo dưỡng, sửa chữa máy chủ, máy trạm, thiết bị công nghệ thông tin bên ngoài cơ quan, phải tháo bỏ bộ phận lưu trữ dữ liệu khỏi thiết bị để lại cơ quan, hoặc phá hủy dữ liệu lưu trữ trên thiết bị.

6. Quản lý sao lưu dự phòng

a) Lập danh sách hệ thống thông tin theo mức độ quan trọng cần được sao lưu kèm tần suất sao lưu, phương pháp sao lưu, thời gian lưu trữ và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu.

b) Dữ liệu của các hệ thống thông tin phải có phương án sao lưu phù hợp với tần suất thay đổi của dữ liệu.

c) Đối với các hệ thống thông tin cấp độ 3 trở lên, dữ liệu sao lưu phải được lưu trữ ra phương tiện lưu trữ ngoài; kiểm tra, phục hồi dữ liệu sao lưu từ phương tiện lưu trữ ngoài đảm bảo an toàn dữ liệu, khả năng phục hồi dữ liệu.

Điều 17. Bảo đảm an toàn thiết bị và người dùng đầu cuối

1. Máy tính cá nhân phải đặt mật khẩu truy cập và chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng; thường xuyên cập nhật bản vá lỗ hổng bảo mật hệ điều hành và phần mềm ứng dụng; cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật mẫu mã độc mới, tự động rà quét khi sao chép, mở các tập tin. Phần mềm phòng chống mã độc phải có tính năng kỹ thuật đáp ứng yêu cầu của Bộ Khoa học và Công nghệ.

2. Khi sử dụng máy tính, thiết bị đầu cuối trong mạng nội bộ cơ quan để xử lý công việc mang tính chất công vụ phải tuân thủ các quy định sau:

a) Không cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn trên máy tính của cơ quan.

b) Cán bộ, công chức, viên chức và người lao động phải tự đặt mật khẩu đăng nhập vào các hệ thống thông tin; thường xuyên thay đổi để tăng cường công tác bảo mật.

c) Không tự ý gỡ bỏ phần mềm phòng chống mã độc trên máy tính. Tất cả các tập tin, thư mục khi sao chép vào máy tính từ thiết bị ngoại vi phải được quét mã độc trước khi thực hiện.

d) Chỉ sử dụng thư điện tử công vụ để trao đổi, gửi, nhận tài liệu công vụ.

e) Khi phát hiện dấu hiệu máy tính nhiễm mã độc phải kịp thời thông báo cho bộ phận có trách nhiệm của cơ quan để xử lý.

3. Cá nhân khi mang máy tính, thiết bị di động thuộc sở hữu riêng kết nối với mạng nội bộ để xử lý công việc phải được sự đồng ý của thủ trưởng cơ quan và tuân thủ các quy định tại Khoản 1, Khoản 2 Điều này.

4. Chấm dứt hoặc thay đổi công việc

a) Cán bộ, công chức, viên chức, người lao động nghỉ việc hoặc thay đổi công việc phải thu hồi các tài khoản, quyền truy cập hệ thống, thiết bị phần cứng, phần mềm và các tài sản công nghệ thông tin khác thuộc sở hữu của cơ quan.

b) Cơ quan có cán bộ, công chức, viên chức, người lao động xin nghỉ việc có trách nhiệm chủ trì, phối hợp với Đơn vị vận hành hệ thống thông tin thu hồi tài khoản, vô hiệu hóa các quyền truy hệ thống. Thời gian thu hồi chậm nhất tối đa sau 05 ngày làm việc.

Chương IV

TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 18. Trách nhiệm của Văn phòng Sở

1. Chủ trì tham mưu các nhiệm vụ về bảo đảm an toàn thông tin mạng trong triển khai các nhiệm vụ ứng dụng công nghệ thông tin và chuyển đổi số phục vụ hoạt động của Sở Nông nghiệp và Môi trường.

2. Chủ trì xây dựng, tham mưu hồ sơ cấp độ an toàn hệ thống thông tin của Sở; hướng dẫn, đôn đốc các đơn vị trực thuộc Sở xây dựng hồ sơ đề xuất cấp độ các hệ thống thông tin do đơn vị vận hành, quản lý.

3. Tham mưu, đề xuất với Lãnh đạo Sở biện pháp quản lý, vận hành; nâng cấp hệ thống mạng nội bộ và triển khai các biện pháp bảo đảm an toàn thông tin đáp ứng nhiệm vụ ứng dụng công nghệ thông tin và chuyển đổi số phục vụ hoạt động của Sở Nông nghiệp và Môi trường.

4. Giám sát, đôn đốc công chức, viên chức, người lao động thực hiện các quy định về đảm bảo an toàn thông tin cấp độ.

5. Hướng dẫn, hỗ trợ, khuyến cáo các rủi ro do mã độc gây ra cho công chức, viên chức, người lao động trong Sở và các đơn vị trực thuộc.

6. Thường xuyên cập nhật các quy định mới về bảo đảm an toàn thông tin mạng trong quá trình vận hành hệ thống; đề xuất phương án bảo đảm an toàn thông tin cho hệ thống mạng và các hệ thống thông tin khi có thay đổi về thiết kế.

7. Định kỳ 02 năm hoặc khi có thay đổi chính sách an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung hệ thống thông tin theo cấp độ.

8. Là đầu mối, phối hợp với các cơ quan chuyên trách để đảm bảo việc xử lý sự cố về an toàn thông tin mạng tại Sở và các đơn vị trực thuộc, đảm bảo kịp thời, hiệu quả và đúng quy định.

9. Cung cấp thông tin, dữ liệu phục vụ thanh tra, kiểm tra, giải quyết khiếu nại, tố cáo về bảo đảm an toàn thông tin khi cấp có thẩm quyền yêu cầu.

10. Tổng hợp và báo cáo về tình hình an toàn thông tin mạng theo định kỳ cho Công an tỉnh, Sở Khoa học và Công nghệ và các cơ quan cấp trên.

Điều 19. Trách nhiệm của các phòng thuộc Sở, các chi cục, các đơn vị sự nghiệp thuộc Sở

1. Trưởng các phòng thuộc Sở, Thủ trưởng cơ quan, đơn vị trực thuộc có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước Sở Nông nghiệp và Môi trường trong công tác bảo đảm an toàn thông tin mạng của phòng, đơn vị mình.

2. Các chi cục, đơn vị sự nghiệp trực thuộc Sở xây dựng ban hành quy chế nội bộ về bảo đảm an toàn thông tin mạng phù hợp với Quy chế này và các quy định của pháp luật.

3. Xây dựng hồ sơ cấp độ của đơn vị, đề nghị cơ quan chuyên trách thẩm định phê duyệt hồ sơ cấp độ hệ thống thông tin của đơn vị theo quy định.

4. Phối hợp, cung cấp thông tin và tạo điều kiện cho các cơ quan, đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố an toàn thông tin mạng kịp thời, nhanh chóng và đạt hiệu quả.

5. Phối hợp chặt chẽ với Văn phòng Sở, các cơ quan chuyên trách Công an tỉnh, Sở Khoa học và Công nghệ và các đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin mạng.

6. Định kỳ 06 tháng (trước ngày 10/7) và hàng năm (trước ngày 10/01 năm tiếp theo) báo cáo tình hình an toàn thông tin mạng của cơ quan theo Mẫu số 03 tại Phụ lục kèm theo Quy chế này, gửi Sở tổng hợp, báo cáo cấp có thẩm quyền.

Điều 20. Trách nhiệm của công chức, viên chức và người lao động trong cơ quan

1. Chấp hành Quy chế này và các quy định của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao.

2. Cán bộ, công chức, viên chức và người lao động có trách nhiệm tự quản lý, bảo quản, bảo đảm an toàn thông tin mạng cho tài khoản, các thiết bị tin học mà mình được giao sử dụng.

3. Khi phát hiện sự cố mất an toàn thông tin mạng phải thông báo ngay với Sở Nông nghiệp và Môi trường, Công an tỉnh, Sở Khoa học và Công nghệ để kịp thời ngăn chặn, xử lý;

4. Tham gia nghiêm túc các chương trình đào tạo, tập huấn về an toàn thông tin mạng, chuyển đổi số do Ủy ban nhân dân tỉnh chỉ đạo hoặc cơ quan chuyên trách (Công an tỉnh, Sở Khoa học và Công nghệ) tổ chức.

Chương V

TỔ CHỨC THỰC HIỆN

Điều 21. Khen thưởng và xử lý vi phạm

1. Việc thực hiện tốt quy chế này là một tiêu chuẩn để bình xét, đánh giá thi đua của mỗi phòng, đơn vị và cá nhân.

2. Các cơ quan, các đơn vị trực thuộc; công chức, viên chức, người lao động có hành vi vi phạm quy định tại quy chế này thì tùy theo tính chất, mức độ vi phạm sẽ xử lý theo quy định của pháp luật.

Điều 22. Tổ chức thực hiện

Chánh Văn phòng Sở, Trưởng các cơ quan, đơn vị trực thuộc tổ chức quán triệt tới công chức, viên chức và người lao động thực hiện Quy chế này. Trong quá trình thực hiện, nếu phát sinh các vấn đề vướng mắc hoặc cần sửa đổi, bổ sung, các phòng, đơn vị kịp thời phản ánh về Văn phòng Sở để tổng hợp, báo cáo Lãnh đạo Sở xem xét, điều chỉnh, bổ sung cho phù hợp./.

Phụ lục

DANH MỤC BIỂU MẪU

(Ban hành kèm theo Quyết định số: /QĐ-SNNMT ngày tháng 9 năm 2025 của Sở Nông nghiệp và Môi trường)

Mẫu số 01	Báo cáo ban đầu sự cố an toàn thông tin mạng
Mẫu số 02	Báo cáo hoàn thành xử lý sự cố an toàn thông tin mạng
Mẫu số 03	Báo cáo định kỳ tình hình an toàn thông tin mạng

(Mẫu số 01)

TÊN CƠ QUAN CHỦ QUẢN **TÊN CƠ QUAN** Số: …../BC-	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc** *Phú Thọ, ngày ... tháng ... năm ...*

BÁO CÁO BAN ĐẦU SỰ CỐ AN TOÀN THÔNG TIN MẠNG

THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN BÁO CÁO SỰ CỐ

- Tên tổ chức/cá nhân báo cáo sự cố (*) .....
- Địa chỉ: (*).....
- Điện thoại (*)..... Email (*) .....

NGƯỜI LIÊN HỆ

- Họ và tên (*) ..... Chức vụ: .....
- Điện thoại (*)..... Email (*).....

THÔNG TIN CHI TIẾT VỀ HỆ THỐNG BỊ SỰ CỐ

Tên đơn vị vận hành hệ thống thông tin (*):	*Điền tên đơn vị vận hành hoặc được thuê vận hành hệ thống thông tin*				
Cơ quan quản lý cấp trên:	*Điền tên cơ quan quản lý cấp trên*				
Tên hệ thống bị sự cố	*Điền tên hệ thống bị sự cố và tên miền, địa chỉ ip liên quan*				
Phân loại cấp độ của hệ thống thông tin, (nếu có)	☐ Cấp độ 1	☐ Cấp độ 2	☐ Cấp độ 3	☐ Cấp độ 4	☐ Cấp độ 5
Tổ chức cung cấp dịch vụ an toàn thông tin mạng (nếu có):	*Điền tên nhà cung cấp ở đây*				
Tên nhà cung cấp dịch vụ kết nối bên ngoài (nếu có)	*Điền tên nhà cung cấp ở đây*				
Dải địa chỉ Public IP kết nối với hệ thống bên ngoài:	*Điền thông tin ở đây*				
Mô tả sơ bộ về sự cố (*)					
Đề nghị cung cấp một bản tóm tắt ngắn gọn về sự cố, bao gồm đánh giá sơ bộ cuộc tấn công đã xảy ra chưa và bất kỳ các nguy cơ dẫn đến khả năng phá hoại hoặc gián đoạn dịch vụ. Xác định mức độ nhạy cảm của thông tin liên quan hoặc những đối tượng bị ảnh hưởng bởi sự cố:.....					

Ngày phát hiện sự cố (*) …/…/….. (dd/mm/yy)	Thời điểm phát hiện (*):	..... giờ.... phút

HIỆN TRẠNG SỰ CỐ (*)

☐ Đã được xử lý

☐ Chưa được xử lý

CÁCH THỨC PHÁT HIỆN * (*Đánh dấu những cách thức được sử dụng để phát hiện sự cố)*

☐ Qua hệ thống phát hiện xâm nhập

☐ Kiểm tra dữ liệu lưu lại (Log File)

☐ Nhận được thông báo từ: .....

☐ Khác, đó là .....

ĐÃ GỬI THÔNG BÁO SỰ CỐ CHO *

☐ Công an tỉnh

☐ Sở Khoa học và Công nghệ

☐ ISP đang trực tiếp cung cấp dịch vụ

☐ Các cơ quan chuyên trách an toàn thông tin mạng khác

THÔNG TIN BỔ SUNG VỀ HỆ THỐNG XẢY RA SỰ CỐ

- Hệ điều hành: ..... Version: .....
- Các dịch vụ có trên hệ thống (*Đánh dấu những dịch vụ được sử dụng trên hệ thống)*

  ☐ Web server ☐ Mail server ☐ Database server

  ☐ Dịch vụ khác, đó là .....
- Các biện pháp an toàn thông tin mạng đã triển khai (*Đánh dấu những biện pháp đã triển khai)*

  ☐ Antivirus

  ☐ Firewall

  ☐ Hệ thống phát hiện xâm nhập

  ☐ Khác: .....
- Các địa chỉ IP của hệ thống *(Liệt kê địa chỉ IP sử dụng trên Internet (IP public), không liệt kê địa chỉ IP nội bộ)*

  .....
- Các tên miền của hệ thống

  .....
- Mục đích chính sử dụng hệ thống.....

  .....
- Thông tin gửi kèm

  ☐ Nhật ký hệ thống

  ☐ Mẫu virus/mã độc

  ☐ Khác: .....
- Các thông tin cung cấp trong thông báo sự cố này đều phải được giữ bí mật:

  ☐ Có ☐ Không

KIẾN NGHỊ, ĐỀ XUẤT HỖ TRỢ

Mô tả về đề xuất, kiến nghị
Đề nghị cung cấp tóm lược về các kiến nghị và đề xuất hỗ trợ ứng cứu (nếu có): …… …… …… ……

THỜI GIAN THỰC HIỆN BÁO CÁO SỰ CỐ *:

.../.../...../.../... (ngày/tháng/năm/giờ/phút)

Nơi nhận:
- Sở NNMT;
- Lưu: VT,....

THỦ TRƯỞNG CƠ QUAN
(Ký số)

***Chú thích**: Phần (*) là những thông tin bắt buộc, các phần còn lại có thể loại bỏ nếu không có thông tin.*

(Mẫu số 02)

TÊN CƠ QUAN CHỦ QUẢN **TÊN CƠ QUAN** Số: …../BC-	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc** *Phú Thọ, ngày ... tháng ... năm ...*

BÁO CÁO HOÀN THÀNH XỬ LÝ SỰ CỐ AN TOÀN THÔNG TIN MẠNG

THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN BÁO CÁO

▪ Tên tổ chức/cá nhân báo cáo sự cố (*) .....

▪ Địa chỉ: (*) .....

▪ Điện thoại (*)……. Email (*).....

VĂN BẢN BÁO CÁO BAN ĐẦU SỰ CỐ:

▪ Số ký hiệu …… Ngày ban hành: …/…/.....

THÔNG TIN CHI TIẾT VỀ HỆ THỐNG BỊ SỰ CỐ

Tên đơn vị vận hành hệ thống thông tin (*):	*Điền tên đơn vị vận hành hoặc được thuê vận hành hệ thống thông tin*				
Cơ quan quản lý cấp trên:	*Điền tên cơ quan quản lý cấp trên*				
Tên hệ thống bị sự cố	*Điền tên hệ thống bị sự cố*				
Phân loại cấp độ của hệ thống thông tin, (nếu có)	☐ Cấp độ 1	☐ Cấp độ 2	☐ Cấp độ 3	☐ Cấp độ 4	☐ Cấp độ 5

Tên/Mô tả về sự cố
Đề nghị cung cấp một bản tóm tắt ngắn gọn về sự cố, bao gồm đánh giá sơ bộ cuộc tấn công đã xảy ra chưa và bất kỳ các nguy cơ dẫn đến khả năng phá hoại hoặc gián đoạn dịch vụ. Xác định mức độ nhạy cảm của thông tin liên quan hoặc những đối tượng bị ảnh hưởng bởi sự cố. (Chỉ mô tả những cập nhật mới có thay đổi so với phần mô tả của văn bản thông báo sự cố đã gửi)

Ngày phát hiện sự cố (*) (dd/mm/yy)	…/…/…..	Thời gian phát hiện (*):	…… giờ ..... phút

Kết quả xử lý sự cố
Cung cấp, tóm tắt tổng quát về những gì đã xảy ra và cách thức giải quyết, đề xuất giải pháp ứng cứu ứng sự cố nhằm xử lý nhanh sự cố, giảm nhẹ rủi ro và thiệt hại đối với sự cố tương tự trong tương lai...

Các tài liệu đính kèm
Liệt kê các tài liệu liên quan (báo cáo diễn biến sự cố; phương án xử lý, log file…..)

Nơi nhận:
- Sở NNMT;
- Lưu: VT,....

THỦ TRƯỞNG CƠ QUAN
(Ký số)

(Mẫu số 03)

TÊN CƠ QUAN CHỦ QUẢN **TÊN CƠ QUAN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: …../BC-	*Phú Thọ, ngày ... tháng ... năm ...*

BÁO CÁO ĐỊNH KỲ TÌNH HÌNH AN TOÀN THÔNG TIN MẠNG

1. Về xây dựng chính sách và biện pháp quản lý an toàn thông tin mạng

a) Đã xây dựng Quy chế bảo đảm an toàn thông tin mạng nội bộ?

❍ Có (*ghi số hiệu văn bản)* ❍ Chưa

b) Đã xây dựng Kế hoạch ứng phó sự cố an toàn thông tin mạng thông thường?

❍ Có *(ghi số hiệu văn bản)* ❍ Không

c) Có bộ phận phụ trách an toàn thông tin mạng?

❍ Có ❍ Không

Nếu có, bộ phận có người phụ trách là:

❍ Lãnh đạo cơ quan

❍ Chuyên viên chuyên trách công nghệ thông tin

❍ Khác: ……

d) Xác định cấp độ an toàn thông tin mạng

- Các hệ thống thông tin đã được phê duyệt cấp độ an toàn thông tin mạng (*liệt kê cụ thể tên hệ thống thông tin, quyết định phê duyệt cấp độ*):

- Các hệ thống thông tin chưa được phê duyệt cấp độ an toàn thông tin mạng (*liệt kê cụ thể tên hệ thống thông tin chưa được phê duyệt*):

đ) Triển khai phương án bảo đảm an toàn thông tin

- Các hệ thống thông tin đã được triển khai phương án bảo đảm an toàn thông tin theo cấp độ (*liệt kê cụ thể tên hệ thống thông tin*):

- Các hệ thống thông tin đã chưa triển khai phương án bảo đảm an toàn thông tin theo cấp độ (*liệt kê cụ thể tên hệ thống thông tin*):

e) Có hệ thống thông tin được lưu ký ngoài Trung tâm dữ liệu tỉnh Phú Thọ?

❍ Có ❍ Không

Nếu có, báo cáo các nội dung sau:

- Tên hệ thống thông tin:

- Đơn vị cung cấp dịch vụ lưu ký (*tên đơn vị, địa chỉ, số điện thoại*):

g) Có thực hiện kiểm định an toàn thông tin mạng đối với hệ thống thông tin mới được xây dựng trong năm?

❍ Có ❍ Không

Nếu có, báo cáo các nội dung sau:

- Tên hệ thống thông tin:

- Đơn vị thực hiện kiểm định (*tên đơn vị, địa chỉ, số điện thoại*):

h) Có thực hiện kiêm tra, đánh giá an toàn thông tin mạng trong năm?

❍ Có ❍ Không

Nếu có, báo cáo các nội dung sau:

- Tên hệ thống thông tin:
- Đơn vị thực hiện đánh giá (*tên đơn vị, địa chỉ, số điện thoại*):
- Các biện pháp đã triển khai xử lý điểm yếu an toàn thông tin:

i) Các công cụ bảo đảm an toàn thông tin mạng đang thực hiện

Công cụ	Tên/phiên bản	Năm đưa vào sử dụng	Mô tả nội dung
1. Phần mềm phòng chống mã độc (antivirus)			
2. Tường lửa			
3. Công cụ mã hóa tập tin			
4. Chữ ký số			
5. Mạng riêng ảo (VPN)			
6. Quản lý Logfile trên thiết bị			
- Thiết bị 1			Nơi lưu trữ
- Thiết bị 2			Nơi lưu trữ
- Thiết bị n			Nơi lưu trữ
7. Quản lý Logfile trên máy chủ			
- Máy chủ 1			Nơi lưu trữ
- Máy chủ 2			Nơi lưu trữ
- Máy chủ n			Nơi lưu trữ
8. Các biện pháp khác:			

2. Về đầu tư cho bảo đảm an toàn thông tin mạng

a) Kinh phí đầu tư cho công tác bảo đảm an toàn thông tin mạng: ..... triệu đồng

b) Tỷ lệ kinh phí trên tổng kinh phí công nghệ thông tin để đầu tư vào việc bảo đảm an toàn thông tin mạng: …….%

c) Đã đầu tư vào lĩnh vực nào dưới đây:

Lĩnh vực	Mô tả nội dung	Kinh phí (đồng)
1. Mua sắm thiết bị, phần mềm chuyên dụng an toàn thông tin mạng	(Mô tả thiết bị, phần mềm)	
2. Mua sắm hệ điều hành, phần mềm bản quyền	(Mô tả hệ điều hành, phần mềm)	
3. Tổ chức đào tạo, tập huấn,	(Mô tả nội dung, thời gian, đối tượng	

hội nghị, hội thảo về an toàn thông tin mạng	đào tạo, tập huấn, hội nghị, hội thảo)	
4. Xây dựng hồ sơ đề xuất cấp độ		
5. Tổ chức kiểm định hệ thống thông tin mới được thiết kế		
6. Tổ chức đánh giá, xử lý rủi ro an toàn thông tin mạng		
7. Tổ chức ứng cứu xử lý sự cố an toàn thông tin mạng		
8. Các lĩnh vực khác:…….		

3. Về phát hiện và xử lý sự cố an toàn thông tin mạng

a) Tổng kết về các sự cố an toàn thông tin mạng đã xảy ra trong năm đối với cơ quan

Sự cố	Số lượng	Biện pháp xử lý
1. Tấn công chiếm quyền điều khiển		
2. Tấn công từ chối dịch vụ		
3. Tấn công mã hóa dữ liệu		
4. Tấn công phá hoại dữ liệu		
5. Tấn công thay đổi giao diện website		
6. Lừa đảo (Phishing)		
7. Thư rác (Spam mail)		
8. Lỗi hạ tầng kỹ thuật, thiết bị, phần mềm		
9. Lỗi quản trị, vận hành		
10. Sự cố khác:		

Biện pháp xử lý: Lựa chọn điền các thông tin sau (1) Không xử lý; (2) Tự xử lý; (3) Báo cáo cơ quan điều phối (Sở TT&TT); (4) Hỗ trợ từ cơ quan khác; (5) Nếu biện pháp khác thì mô tả cụ thể.

b) Mức độ thiệt hại trong năm 20... do các sự cố an toàn thông tin mạng gây ra

☐ Thiệt hại gián tiếp: …… triệu đồng

☐ Thiệt hại trực tiếp: …… triệu đồng

☐ Chi phí khắc phục: …… triệu đồng

c) Công việc cơ quan đã thực hiện sau khi khắc phục được sự cố trong năm qua

☐ Liên kết, để được hỗ trợ từ các đơn vị hoạt động trong lĩnh vực an toàn thông tin mạng

☐ Sửa đổi chính sách/hướng dẫn/thủ tục

☐ Nâng cao ý thức; ☐ Tăng cường thiết bị

☐ Rà soát lại hệ thống; ☐ Công việc khác (*mô tả cụ thể*):

……..

……..

……..

……..

4. Kiến nghị, đề xuất

……..

……..

……..

……..

Nơi nhận:
- Sở NNMT;
- Lưu VT.

THỦ TRƯỞNG CƠ QUAN
(Ký số)

***Ghi chú**:*

- Điền thông tin đầy đủ vào các câu hỏi: Để lựa chọn đánh dấu X

- Câu hỏi với ký hiệu ❍ trước mỗi lựa chọn thì chỉ được phép đánh dấu một kết quả (chọn một)

- Câu hỏi với ký hiệu ☐ trước mỗi lựa chọn thì có thể đánh dấu từ không tới nhiều kết quả (chọn nhiều)

- Ký số và gửi liên thông về Công an tỉnh, Sở Khoa học và Công nghệ.