UBND TỈNH VĨNH PHÚC **SỞ THÔNG TIN VÀ TRUYỀN THÔNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số:304 /QĐ-STTTT	*Vĩnh Phúc, ngày 04 tháng 11 năm 2022*

QUYẾT ĐỊNH

Ban hành Quy định bảo đảm an toàn thông tin mạng trong triển khai các nhiệm vụ chuyển đổi số phục vụ hoạt động của Sở Thông tin và Truyền thông

GIÁM ĐỐC SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Căn cứ Luật An toàn thông tin mạng ngày 19/11/2015;

Căn cứ Luật An ninh mạng ngày 12/6/2018;

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

Căn cứ Quyết định số 31/2018/QĐ-UBND ngày 17/12/2018 của UBND tỉnh Vĩnh Phúc về việc ban hành Quy định bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước tỉnh Vĩnh Phúc;

Căn cứ Quyết định số 4005/2016/QĐ-UBND ngày 09/12/2016 của UBND tỉnh Vĩnh Phúc về việc Quy định vị trí, chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Thông tin và Truyền thông; Quyết định số 37/2019/QĐ-UBND ngày 08/8/2019 của UBND tỉnh Vĩnh Phúc sửa đổi khoản 2, Điều 3 Quyết định số 4005/2016/QĐ-UBND ngày 09/12/2016;

Theo đề nghị của Giám đốc Trung tâm Hạ tầng thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy định bảo đảm an toàn thông tin mạng trong triển khai các nhiệm vụ chuyển đổi số phục vụ hoạt động của Sở Thông tin và Truyền thông.

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

Điều 3. Chánh Văn phòng, Trưởng các phòng, đơn vị; công chức, viên chức, người lao động và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như điều 3;
- Giám đốc và các PGĐ;
- Lưu: VT, TTHTTT.

GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH VĨNH PHÚC

Nguyễn Bá Hiến

UBND TỈNH VĨNH PHÚC
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

QUY ĐỊNH

Bảo đảm an toàn thông tin mạng trong triển khai các nhiệm vụ chuyển đổi số phục vụ hoạt động của Sở Thông tin và Truyền thông

(Kèm theo Quyết định số /QĐ-STTTT ngày tháng 11 năm 2022 của Giám đốc Sở Thông tin và Truyền thông)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Quy định này quy định về việc bảo đảm an toàn thông tin mạng trong quá trình triển khai các nhiệm vụ chuyển đổi số phục vụ hoạt động của Sở Thông tin và Truyền thông.

2. Quy định này được áp dụng với công chức, viên chức và người lao động thuộc Sở Thông tin và Truyền thông.

3. Quy định này không áp dụng đối với công tác quản lý, vận hành và bảo đảm an toàn thông tin cho các hệ thống thông tin tại Trung tâm dữ liệu của tỉnh.

Điều 2. Giải thích từ ngữ

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

1. *An toàn thông tin mạng* được quy định tại Khoản 1, Điều 3, Luật An toàn thông tin mạng.

2. *Hệ thống thông tin* được quy định tại Khoản 3, Điều 3, Luật An toàn thông tin mạng.

3. *Hạ tầng kỹ thuật* được quy định tại Khoản 7, Điều 3, Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về Ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước.

Điều 3. Mục tiêu, nguyên tắc bảo đảm an toàn thông tin mạng

1. Mục tiêu: Để bảo đảm an toàn thông tin mạng trong triển khai các nhiệm vụ chuyển đổi số phục vụ hoạt động của Sở Thông tin và Truyền thông.

2. Nguyên tắc

a) Triển khai các nhiệm vụ chuyển đổi số phục vụ hoạt động của Sở Thông tin và Truyền thông phải tuân theo nguyên tắc bảo đảm an toàn thông tin được quy định tại Điều 4, Luật An toàn thông tin mạng ngày 19/11/2015.

b) Bảo đảm an toàn thông tin là yêu cầu bắt buộc trong triển khai các nhiệm vụ chuyển đổi số phục vụ hoạt động của Sở Thông tin và Truyền thông. Bao gồm: thu thập, tạo lập, xử lý, truyền tải, lưu trữ và sử dụng thông tin, dữ liệu; thiết kế, vận hành, nâng cấp, hủy bỏ hệ thống thông tin.

Điều 4. Các hành vi nghiêm cấm

Các hành vi bị nghiêm cấm về an toàn, an ninh thông tin mạng theo quy định tại Điều 7, Luật An toàn thông tin mạng và Điều 8, Luật An ninh mạng.

Điều 5. Tổ chức bảo đảm an toàn thông tin

1. Phòng Công nghệ thông tin là Bộ phận chuyên trách về an toàn thông tin mạng của Sở Thông tin và Truyền thông; thực hiện các chức năng của Bộ phận chuyên trách về an toàn thông tin mạng theo quy định của Pháp luật.

2. Trung tâm Hạ tầng thông tin là Đơn vị chịu trách nhiệm vận hành hệ thống mạng của Tòa nhà Sở Thông tin và Truyền thông; thực thi, triển khai các biện pháp bảo đảm an toàn thông tin trong cho các hệ thống thông tin của Sở Thông tin và Truyền thông; Là đầu mối của Sở Thông tin và Truyền thông trong tiếp nhận, hỗ trợ, hướng dẫn; phối hợp xử lý, điều phối ứng cứu sự cố an toàn thông tin mạng.

Điều 6. Bảo đảm nguồn nhân lực

1. Tuyển dụng

Công chức, viên chức, người lao động tuyển dụng hoặc sắp xếp, giao nhiệm vụ về an toàn thông tin có trình độ, chuyên ngành phù hợp yêu cầu đối với các vị trí việc làm về công nghệ thông tin, an toàn thông tin theo hướng dẫn của Bộ Thông tin và Truyền thông.

2. Quá trình làm việc

a) Công chức, viên chức và người lao động cơ quản phải tuân thủ quy định này và các quy định khác của pháp luật có liên quan về bảo đảm an toàn thông tin mạng; tham gia đầy đủ các chương trình đào tạo nâng cao nhận thức về an toàn thông tin mạng của Sở Thông tin và Truyền thông khi được triệu tập.

b) Các thông tin tuyên truyền, phổ biến kiến thức về an toàn thông tin phải được phổ biến đến 100% công chức, viên chức và người lao động trong cơ quan trên Phần mềm Quản lý văn bản và Điều hành.

3. Chấm dứt hoặc thay đổi công việc

a) 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, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của cơ quan.

b) Văn phòng Sở, Trưởng các phòng, Giám đốc các đơn vị trực thuộc có trách nhiệm phối hợp với Trung tâm Hạ tầng thông tin trong việc thù hồi tài sản, tài khoản, quyền truy cập của công chức, viên chức và người lao động nghỉ việc.

Chương II
BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ THIẾT KẾ XÂY DỰNG HỆ THỐNG THÔNG TIN

Điều 7. Thiết kế an toàn hệ thống thông tin

1. Đơn vị được giao chủ trì xây dựng mới hệ thống thông tin có trách nhiệm phối hợp đơn vị tư vấn triển khai xây dựng hồ sơ đề xuất cấp độ an toàn hệ thống thông tin và phương án bảo đảm an toàn thông tin theo cấp độ để triển khai đồng thời cùng quá trình triển khai dự án theo đúng quy định của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Khi hệ thống thông tin có thay đổi thiết kế cần đánh giá lại tính phù hợp của phương án bảo đảm an toàn thông tin để kịp thời sửa đổi, bổ sung.

3. Trường hợp hệ thống được xây dựng theo hình thức thuê khoán, trong hợp đồng thuê phải có các điều khoản liên quan đến bảo đảm an toàn hệ thống thông tin theo cấp độ.

Điều 8. Thử nghiệm và nghiệm thu hệ thống

1. Khi phát triển phần mềm nội bộ, đối với các hệ thống thông tin yêu cầu bắt buộc phải kiểm thử theo quy định của Pháp luật, trước khi đưa vào sử dụng phải được kiểm thử để bảo đảm an toàn thông tin. Đơn vị chủ trì có trách nhiệm yêu cầu đơn vị phát triển cung cấp mã nguồn phần mềm.

2. Các hệ thống hạ tầng kỹ thuật khác phải được vận hành thử, nghiệm thu trước khi đưa vào sử dụng. Đơn vị chủ trì có trách nhiệm phối hợp với tư vấn triển khai và các tổ chức, cá nhân liên quan tổ chức vận hành thử và nghiệm thu.

Chương III
BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ VẬN HÀNH HỆ THỐNG

Điều 9. Quản lý an toàn mạng

1. Công chức, viên chức và người lao động trong cơ quan khi sử dụng máy tính trong mạng nội bộ không được tự ý thay đổi địa chỉ IP và địa chỉ Default gateway đã được cấp mặc định.

2. Không được tự ý lắp đặt các thiết bị thu, phát sóng Wifi (Access Point, Router Wifi) vào mạng khi chưa thống nhất với Đơn vị vận hành mạng nội bộ.

3. Thiết bị mạng không dây trong mạng nội bộ phải được đặt mật khẩu truy cập, thường xuyên thay đổi; sao lưu các tập tin cấu hình hệ thống của các thiết bị quan trọng để sẵn sàng khôi phục khi xảy ra sự cố.

4. Không cung cấp mật khẩu của các thiết bị phát sóng Wifi trong mạng nội bộ ra bên ngoài, trừ các đoàn công tác đến làm việc trực tiếp với đơn vị.

5. Việc sử dụng mạng riêng ảo (VPN - Virtual Private Network) khi có nhu cầu làm việc từ xa, bắt buộc phải đặt mật khẩu với độ an toàn cao theo quy định tại Khoản 7, Điều 10 và thay đổi mật khẩu tối thiểu 03 lần/tháng.

6. Hạn chế tối đa sử dụng chức năng chia sẻ tài nguyên trên các máy tính cá nhân (sharing), trừ máy in. Trường hợp cần thiết sử dụng chức năng này, bắt buộc phải thiết lập mật khẩu và thực hiện việc thu hồi chức năng này khi đã sử dụng xong.

Điều 10. Quản lý an toàn máy chủ và ứng dụng

1. Bảo đảm cho mạng kết nối đến máy chủ, hệ điều hành trên máy chủ, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn.

2. Không cài đặt các phần mềm không liên quan đến hệ thống thông tin trên máy chủ cài đặt hệ thống thông tin.

3. Máy chủ phải thường xuyên được thiết lập tự động cập nhật các bản vá lỗi hệ điều hành của nhà sản xuất. Nhật ký máy chủ phải lưu trữ ít nhất 01 tháng.

4. Phải thay đổi tài khoản, mật khẩu mặc định khi đưa hệ điều hành trên máy chủ vào sử dụng. Loại bỏ các tài khoản không còn sử dụng khỏi máy chủ.

5. Mỗi tài khoản truy cập các hệ thống thông tin chỉ được cấp cho một người quản lý và sử dụng. Người sử dụng phải có trách nhiệm bảo vệ tài khoản truy cập của mình.

Điều 11. Quản lý an toàn dữ liệu

1. Các phòng, đơn vị được giao chủ trì quản lý, sử dụng hệ thống thông tin nào có trách nhiệm tự sao lưu dữ liệu cá nhân phục vụ công tác chuyên môn.

2. Với các dữ liệu của hệ thống thông tin nghiệp vụ dùng chung trong toàn cơ quan, Trung tâm Hạ tầng thông tin có trách nhiệm sao lưu dự phòng vào thiết bị lưu trữ chuyên dụng.

3. Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ và các dữ liệu quan trọng khác trên hệ thống (nếu có).

Điều 12. Quản lý an toàn người sử dụng đầu cuối

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

2. Máy trạm phải được đặt mật khẩu truy cập và thiết lập chế độ tự động bảo vệ màn hình sau 15 phút không sử dụng. Trường hợp không sử dụng trong thời gian quá 02 giờ trở lên phải tắt máy để bảo đảm an toàn.

3. Mỗi công chức, viên chức và người lao động phải tự đặt mật khẩu đăng nhập vào các hệ thống thông tin có độ phức tạp cao (có độ dài tối thiểu 8 ký tự,

có ký tự thường, ký tự hoa, ký tự số và ký tự đặc biệt như !, @, #, $, %,...) và thường xuyên thay đổi để tăng cường công tác bảo mật.

4. Công chức, viên chức và người lao động có trách nhiệm triển khai các biện pháp phòng chống mã độc theo hướng dẫn của Đơn vị vận hành mạng nội bộ.

5. Không tự ý gỡ bỏ các phần mềm phòng chống mã độc trên máy tính. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật. 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.

6. Không truy cập vào các hệ thống thông tin công cộng không rõ về nội dung hoặc có nội dung phản cảm, không phù hợp với thuần phong mỹ tục của Việt Nam. Không đọc thư điện tử hoặc tải tệp tin đính kèm trong thư không rõ người gửi; Không kích hoạt các đường liên kết có dấu hiệu không rõ ràng.

Điều 13. Quản lý sự cố

1. Phân loại mức độ nghiêm trọng của các sự cố, bao gồm:

a) Thấp: Sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của các phòng, đơn vị thuộc Sở Thông tin và Truyền thông.

b) Trung bình: Sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoán hay đình trệ hoạt động chính của các phòng, đơn vị thuộc Sở Thông tin và Truyền thông.

c) Cao: Sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và gây ảnh hưởng đến một trong các hoạt động chính của các phòng, đơn vị thuộc Sở Thông tin và Truyền thông.

d) Nghiêm trọng: Sự cố ảnh hưởng liên tục đến nhiều hoạt động chính của các phòng, đơn vị thuộc Sở Thông tin và Truyền thông.

2. Xử lý sự cố:

a) Khi có sự cố tại Điểm a, b, Khoản 1 Điều này, công chức, viên chức, người lao động có trách nhiệm báo với Đơn vị vận hành mạng nội bộ để để kịp thời xử lý.

b) Khi có sự cố tại Điểm c, Khoản 1 Điều này, công chức, viên chức, người lao động có trách nhiệm báo với Đơn vị vận hành mạng nội bộ và Giám đốc Sở để xin ý kiến chỉ đạo xử lý kịp thời.

c) Đối với sự cố quy định tại Điểm d, Khoản 1 Điều này, Đơn vị vận hành mạng nội bộ báo cáo Giám đốc Sở và triển khai quy trình ứng cứu theo Quy định tại Điều 12, Quyết định số 31/2018/QĐ-UBND ngày 17/12/2018 của UBND tỉnh Vĩnh Phúc ban hành Quy định bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước tỉnh Vĩnh Phúc.

3. Trung tâm Hạ tầng thông tin có trách nhiệm tham mưu chính sách, quy trình quản lý sự cố an toàn thông tin.

Điều 14. Kiểm tra, đánh giá và quản lý rủi do

1. Nội dung kiểm tra, đánh giá và quản lý rủi ro an toàn thông tin

a) Kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ.

b) Đánh giá hiệu quả của biện pháp bảo đảm an toàn hệ thống thông tin.

c) Đánh giá phát hiện mã độc, lỗ hổng hệ thống.

d) Kiểm tra, đánh giá khác do chủ quản hệ thống thông tin quy định.

2. Hình thức kiểm tra, đánh giá và quản lý rủi ro an toàn thông tin

a) Định kỳ theo kế hoạch của chủ quản hệ thống thông tin.

b) Kiểm tra, đánh giá đột xuất theo yêu cầu của cấp có thẩm quyền.

Điều 15. 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, thanh hủy tài sản.

Chương III
TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 16. Trách nhiệm của phòng Công nghệ thông tin

1. Chủ trì tham mưu các nhiệm vụ về bảo đảm an toàn thông mạng trong triển khai các nhiệm vụ chuyển đổi số phục vụ hoạt động của Sở Thông tin và Truyền thông.

2. Chủ trì chỉ đạo, đôn đốc, hướng dẫn và tham mưu thẩm định hồ sơ cấp độ an toàn hệ thống thông tin của các hệ thống thông tin do đơn vị vận hành hệ thống đề xuất triển khai.

3. Phối hợp với Trung tâm Hạ tầng thông tin triển khai quy định này.

Điều 17. Trách nhiệm của Trung tâm Hạ tầng thông tin

1. Chủ trì phối hợp với phòng Công nghệ thông tin triển khai quy định này.

2. 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 chuyển đổi số phục vụ hoạt động của Sở Thông tin và Truyền thông.

3. Giám sát, nhắc nhở công chức, viên chức, người lao động thay đổi mật khẩu thường xuyên.

4. Hướng dẫn, hỗ trợ, khuyến cáo các rủi ro do mã độc gây ra cho công chức, viên chức, người lao động trong toàn cơ quan.

5. 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.

6. Định kỳ 03 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.

7. 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.

Điều 18. Trách nhiệm của các phòng, đơn vị sự nghiệp thuộc Sở

1. Trưởng các phòng, Thủ trưởng đơn các vị sự nghiệp có trách nhiệm tổ chức thực hiện Quy định này và chịu trách nhiệm trong công tác bảo đảm an toàn thông tin của phòng, đơn vị mình.

2. Thường xuyên quán triệt các quy định về an toàn thông tin mạng để nâng cao nhận thức về trách nhiệm bảo đảm an toàn thông tin.

3. Cử cán bộ đầu mối phối hợp với Trung tâm Hạ tầng thông tin theo dõi, xử lý các sự cố an toàn thông tin của phòng, đơn vị và trong toàn cơ quan.

4. Phối hợp, cung cấp thông tin và tạo điều kiện để Trung tâm Hạ tầng thông tin hoặc các đơn vị có thẩm quyền triển khai công tác kiểm tra, khắc phục sự cố an toàn thông tin kịp thời, nhanh chóng và đạt hiệu quả.

Điều 19. Trách nhiệm của công chức và người lao động trong cơ quan

1. Nghiêm túc chấp hành quy định này và các quy định khác của pháp luật về an toàn thông tin. Chịu trách nhiệm bảo đảm an toàn thông tin trong phạm vi trách nhiệm và quyền hạn được giao.

2. Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin phải báo cáo ngay với cấp trên và Trung tâm Hạ tầng thông tin để kịp thời ngăn chặn và xử lý.

3. Tham gia đầy đủ các chương trình diễn tập, tập huấn về an toàn thông tin mạng do Sở Thông tin và Truyền thông, Bộ Thông tin và Truyền thông tổ chức.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 20. Khen thưởng và xử lý vi phạm

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

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

Điều 21. Tổ chức thực hiện

Trưởng phòng, Thủ trưởng các đơn vị trực thuộc tổ chức quán triệt tới công chức, viên chức và người lao động thực hiện Quy định 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 Trung tâm Hạ tầng thông tin để tổng hợp, báo cáo Lãnh đạo Sở xem xét, điều chỉnh, bổ sung cho phù hợp./.