

Từ Sơn, ngày 28 tháng 9 năm 2021

Số: 1097/QĐ-BCĐ

QUYẾT ĐỊNH

Ban hành Quy chế đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của các cơ quan Nhà nước trên địa bàn thị xã Từ Sơn

TRƯỞNG BAN BAN CHỈ ĐẠO XÂY DỰNG CHÍNH QUYỀN ĐIỆN TỬ THỊ XÃ TỪ SƠN

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19/6/2015;

Căn cứ Nghị quyết số 36/NQ-TW ngày 01/7/2014 của Bộ Chính trị về đẩy mạnh ứng dụng, phát triển công nghệ thông tin đáp ứng yêu cầu phát triển bền vững và hội nhập quốc tế;

Căn cứ Quyết định số 74/QĐ-UBND ngày 20/01/2021 của UBND tỉnh Bắc Ninh về việc kiện toàn Ban Chỉ đạo xây dựng Chính quyền điện tử tỉnh Bắc Ninh;

Căn cứ Quyết định số 1031/QĐ-UBND ngày 23/9/2021 của Chủ tịch UBND thị xã về việc thành lập Ban Chỉ đạo xây dựng chính quyền điện tử thị xã Từ Sơn;

Xét đề nghị của Trưởng phòng Văn hoá và Thông tin,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo quyết định này bản Quy chế đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của các cơ quan Nhà nước trên địa bàn thị xã Từ Sơn

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

Thủ trưởng các cơ quan: Văn phòng HĐND - UBND thị xã; các phòng, ban, đơn vị trực thuộc UBND thị xã; Chủ tịch UBND các phường; Thành viên Ban Chỉ đạo xây dựng chính quyền điện tử thị xã Từ Sơn, các cơ quan, đơn vị có liên quan chịu trách nhiệm thi hành quyết định này./.

Nơi nhận:

- BCĐ XDCQĐT tỉnh (b/c);
- TT. TU, HĐND thị xã (b/c);
- Chủ tịch, các PCT UBND thị xã;
- Các cơ quan, ban, ngành thị xã;
- Thành viên BCĐ XDCQĐT thị xã;
- UBND phường;
- Lưu VT, VHHT.

TRƯỞNG BAN

**CHỦ TỊCH UBND THỊ XÃ
Hoàng Bá Huy**

QUY CHẾ

**Về đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực CNTT
trong hoạt động của các cơ quan Nhà nước trên địa bàn thị xã Từ Sơn**
(Ban hành kèm theo Quyết định số: 1097/QĐ-BCĐCQĐT ngày 28/9/2021
của Ban Chỉ đạo xây dựng chính quyền điện tử thị xã Từ Sơn)

Chương I

QUY ĐỊNH CHUNG

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

1. Quy chế này quy định về công tác đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước, đơn vị sự nghiệp trên địa bàn thị xã Từ Sơn (sau đây gọi tắt là cơ quan).

2. Quy chế này được áp dụng đối với các các tổ chức, cá nhân liên quan đến an toàn, an ninh thông tin trong các cơ quan nhà nước, đơn vị sự nghiệp trên địa bàn thị xã Từ Sơn.

Điều 2. Mục đích, nguyên tắc đảm bảo an toàn, an ninh thông tin

1. Việc áp dụng Quy chế này nhằm giảm thiểu được các nguy cơ gây mất an toàn thông tin và đảm bảo an ninh thông tin trong quá trình ứng dụng công nghệ thông tin trong hoạt động của các cơ quan.

2. Các hoạt động ứng dụng công nghệ thông tin phải tuân theo nguyên tắc đảm bảo an toàn thông tin được quy định tại Điều 41, Nghị định 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước.

Chương II

QUY ĐỊNH ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 3. Về quản lý cán bộ, công chức và viên chức

1. Các cơ quan phải xây dựng các yêu cầu, trách nhiệm đảm bảo an toàn thông tin đối với từng vị trí công việc. Trước khi tiếp nhận nhân sự, các cơ quan phải kiểm tra khả năng đáp ứng các yêu cầu về an toàn thông tin của nhân sự mới. Trong các hợp đồng lao động, phải có các điều khoản về trách nhiệm đảm bảo an toàn thông tin.

2. Các cơ quan phải thường xuyên tổ chức quán triệt các quy định về an toàn thông tin, nhằm nâng cao nhận thức về trách nhiệm đảm bảo an toàn thông tin của từng cá nhân trong cơ quan.

3. Hủy tài khoản, quyền truy cập các hệ thống thông tin, thu hồi lại tất cả các tài sản liên quan tới hệ thống thông tin (khoá, thẻ nhận dạng, thư mục lưu trữ, thư điện tử, máy vi tính, ...) đối với các cá nhân nghỉ việc, chuyển công tác.

Điều 4. Quản lý phòng máy chủ

1. Các thiết bị mạng quan trọng như tường lửa (firewall), thiết bị định tuyến (router), hệ thống máy chủ, ... phải được đặt trong phòng máy chủ và có các biện pháp bảo vệ, ngăn chặn xâm nhập trái phép vào phòng máy chủ.

2. Phòng máy chủ của các cơ quan là khu vực hạn chế tiếp cận và được lắp đặt hệ thống camera giám sát. Chỉ những người có trách nhiệm theo quy định của thủ trưởng cơ quan mới được phép vào phòng máy chủ.

3. Quá trình vào, ra phòng máy chủ phải được ghi nhận vào nhật ký quản lý phòng máy chủ.

4. Phòng máy chủ phải có hệ thống lưu điện đủ công suất và duy trì thời gian hoạt động của các máy chủ tối thiểu 15 phút khi có sự cố mất điện.

Điều 5. Phòng chống mã độc

1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống mã độc. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin.

2. Các cán bộ, công chức và viên chức trong cơ quan phải được hướng dẫn về phòng chống mã độc, các rủi ro do mã độc gây ra; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm trên máy trạm khi chưa có sự đồng ý của người có thẩm quyền theo quy định của cơ quan.

3. Tất cả các máy tính của đơn vị phải được cấu hình nhằm vô hiệu hóa tính năng tự động thực thi (autoplay) các tập tin trên các thiết bị lưu trữ di động.

4. Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng.

5. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu,...), người sử dụng phải tắt máy và báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý.

Điều 6. Sao lưu dữ liệu dự phòng

1. Các dữ liệu quan trọng của cơ quan phải được sao lưu, bao gồm: thông tin cấu hình của hệ thống mạng, máy chủ; phần mềm ứng dụng và cơ sở dữ liệu; tập tin ghi nhật ký.

2. Các cơ quan phải lập kế hoạch và thực hiện sao lưu dữ liệu phù hợp với điều kiện của từng cơ quan, đảm bảo khả năng phục hồi dữ liệu khi có sự cố xảy ra.

Điều 7. Quản lý thiết bị tường lửa

1. Các hạ tầng công nghệ thông tin phải được trang bị tường lửa để ngăn chặn và phát hiện các xâm nhập trái phép vào mạng nội bộ.

2. Nhật ký hoạt động của thiết bị tường lửa phải được lưu giữ an toàn để phục vụ công tác khảo sát, điều tra khi có sự cố xảy ra.

Điều 8. Quản lý nhật ký trong quá trình vận hành các hệ thống thông tin

1. Các cơ quan phải thực hiện việc ghi nhật ký (log) trên các thiết bị mạng máy tính, phần mềm ứng dụng, hệ điều hành, cơ sở dữ liệu nhằm đảm bảo các sự kiện quan trọng xảy ra trên hệ thống được ghi nhận và lưu giữ.

2. Các nhật ký này phải được bảo vệ an toàn nhằm phục vụ công tác kiểm tra, phân tích khi cần thiết.

3. Các sự kiện tối thiểu cần phải được ghi nhật ký gồm: quá trình đăng nhập hệ thống; tạo, cập nhật hoặc xóa dữ liệu; các hành vi xem, thiết lập cấu hình hệ thống; việc thiết lập các kết nối bất thường vào và ra hệ thống; thay đổi quyền truy cập hệ thống.

4. Thường xuyên thực hiện việc theo dõi bản ghi nhật ký của hệ thống và các sự kiện khác có liên quan để đánh giá, báo cáo các rủi ro và mức độ nghiêm trọng các rủi ro đó.

Điều 9. Quản lý truy cập

1. Các quy định về quản lý truy cập vào hệ thống thông tin, mạng máy tính, thiết bị, phần mềm ứng dụng của đơn vị phải được quy định chi tiết và tổ chức thực hiện nghiêm túc, phù hợp với các quy định của pháp luật về an toàn thông tin.

2. Mỗi tài khoản truy cập các hệ thống thông tin chỉ được cấp cho một người quản lý và sử dụng.

3. Mỗi cán bộ, công chức và viên chức chỉ được phép truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình, có trách nhiệm bảo mật tài khoản truy cập thông tin.

4. Các hệ thống thông tin cần giới hạn số lần đăng nhập sai liên tiếp vào hệ thống. Hệ thống tự động khoá tài khoản trong một khoảng thời gian nhất định trước khi tiếp tục cho đăng nhập nếu liên tục đăng nhập sai vượt quá số lần quy định.

5. Tất cả máy trạm, máy chủ phải được đặt mật khẩu truy cập và thiết lập chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng.

6. Khi thiết lập mạng không dây trong nội bộ đơn vị, phải đặt mật khẩu truy cập vào mạng không dây và chỉ cho phép truy cập Internet.

7. Mật khẩu đăng nhập vào các hệ thống thông tin phải có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự số và ký tự đặc biệt như !, @, #, \$, %, ...) và phải được thay đổi ít nhất 3 tháng/lần.

Điều 10. Quản lý sự cố

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

1.1. Thấp: sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan;

1.2. Trung bình: sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của đơn vị;

1.3. 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 cơ quan;

1.4. Khẩn cấp: sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của cơ quan.

2. Khi có sự cố hoặc nguy cơ mất an toàn thông tin thì lãnh đơn vị phải chỉ đạo kịp thời để khắc phục và hạn chế thiệt hại, báo cáo bằng văn bản cho cơ quan cấp trên trực tiếp quản lý và Phòng Văn hóa và Thông tin.

3. Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của đơn vị, lãnh đạo đơn vị phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và Phòng Văn hóa và Thông tin để được hướng dẫn, hỗ trợ.

Điều 11. Các hành vi bị nghiêm cấm

1. Cài đặt thêm các chương trình, phần mềm, can thiệp vào phần cứng và phần mềm cài đặt sẵn, tự ý dịch chuyển, tháo lắp các trang thiết bị mà không có sự đồng ý của cấp có thẩm quyền;

2. Xâm nhập, sửa đổi, xóa bỏ nội dung thông tin của cơ quan, cá nhân khác.

3. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin.

4. Ngăn chặn việc truy nhập đến thông tin của cơ quan, cá nhân khác trên môi trường mạng, trừ trường hợp pháp luật cho phép.

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

6. 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 III

TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 12. Trách nhiệm của cán bộ, công chức, viên chức trong các cơ quan

1. Trách nhiệm của người phụ trách an toàn thông tin:

1.1. Chịu trách nhiệm đảm bảo an toàn thông tin của đơn vị;

1.2. Tham mưu lãnh đạo cơ quan ban hành các quy định, quy trình nội bộ, triển khai các giải pháp kỹ thuật đảm bảo an toàn thông tin;

1.3. Thực hiện việc giám sát, đánh giá, báo cáo thủ trưởng cơ quan các rủi ro mất an toàn thông tin và mức độ nghiêm trọng của các rủi ro đó;

1.4. Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn, an ninh thông tin.

2. Trách nhiệm của cán bộ, công chức, viên chức trong các cơ quan, đơn vị:

2.1. Nghiêm túc chấp hành các quy định, quy trình nội bộ, Quy chế này và các quy định khác của pháp luật về an toàn thông tin. Chịu trách nhiệm đảm bảo an toàn thông tin trong phạm vi trách nhiệm và quyền hạn được giao;

2.2. Mỗi cán bộ, công chức và viên chức phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp các thiết bị trên máy tính; không được vào các trang web không rõ về nội dung; không tải và cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn; không nhấp chuột vào các đường dẫn lạ không rõ về nội dung;

2.3. Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin phải báo cáo ngay với cấp trên và bộ phận chuyên trách công nghệ thông tin của đơn vị để kịp thời ngăn chặn và xử lý;

2.4. Tham gia các chương trình đào tạo, hội nghị về an toàn an ninh thông tin do cơ quan hoặc Phòng Văn hóa và Thông tin tổ chức.

Điều 13. Trách nhiệm của các cơ quan

1. Thủ trưởng các cơ quan, đơn vị có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước UBND thị xã trong công tác đảm bảo an toàn thông tin của đơn vị mình.

2. Phân công một bộ phận hoặc cán bộ chuyên trách đảm bảo an toàn thông tin của đơn vị; tạo điều kiện để các cán bộ phụ trách an toàn thông tin được học tập, nâng cao trình độ về an toàn thông tin.

3. Xây dựng quy định, quy trình nội bộ về đảm bảo an toàn thông tin phù hợp với Quy chế này và các quy định của pháp luật.

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

5. Phối hợp chặt chẽ với Công an thị xã trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn, an ninh thông tin.

6. Định kỳ hàng quý, các cơ quan lập báo cáo về tình hình an toàn thông tin và gửi về Phòng Văn hóa và Thông tin để tổng hợp báo cáo UBND thị xã.

Điều 14. Trách nhiệm của Phòng Văn hóa và Thông tin

1. Tham mưu UBND thị xã về công tác đảm bảo an toàn, an ninh thông tin trên địa bàn thị xã. Hàng năm, xây dựng kế hoạch triển khai công tác đảm bảo an toàn thông tin phục vụ cho việc vận hành các hệ thống thông tin được UBND thị xã giao quản lý.

2. Chủ trì, phối hợp với Công an thị xã và các cơ quan, đơn vị liên quan tổ chức kiểm tra theo định kỳ hoặc đột xuất; kịp thời phát hiện và xử lý theo quy định của pháp luật đối với các cơ quan, tổ chức, cá nhân có các dấu hiệu, hành vi vi phạm an toàn, an ninh thông tin trên địa bàn thị xã.

3. Xây dựng và triển khai các chương trình đào tạo chuyên sâu về an toàn, an ninh thông tin cho lực lượng đảm bảo an toàn, an ninh thông tin của các cơ quan, đơn vị.

4. Tổ chức các hội nghị, hội thảo chuyên đề và tuyên truyền về an toàn, an ninh thông tin trong công tác quản lý Nhà nước trên địa bàn thị xã.

5. Tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin.

6. Hướng dẫn, giám sát các cơ quan, đơn vị trên địa bàn thị xã xây dựng quy chế nội bộ và thực hiện việc đảm bảo an toàn, an ninh cho hệ thống thông tin theo quy định của Nhà nước.

7. Tổng hợp và báo cáo về tình hình an toàn, an ninh thông tin theo định kỳ cho UBND thị xã, Sở Thông tin và Truyền thông tỉnh Bắc Ninh.

Điều 15. Trách nhiệm của Công an thị xã

1. Chủ trì, phối hợp với Phòng Văn hóa và Thông tin, các cơ quan, đơn vị có liên quan xây dựng kế hoạch và chịu trách nhiệm kiểm soát, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm lợi dụng hệ thống thông tin gây hại đến an toàn, an ninh thông tin trong cơ quan nhà nước.

2. Phối hợp với các cơ quan chức năng trong trao đổi biện pháp kỹ thuật, kiểm tra, đánh giá nhằm đảm bảo an toàn, an ninh thông tin.

3. Tăng cường công tác phòng ngừa, phát hiện và tuyên truyền, phổ biến pháp luật về xử lý tội phạm trong việc đảm bảo an toàn, an ninh thông tin.

4. Điều tra và xử lý các trường hợp vi phạm pháp luật về an toàn, an ninh thông tin theo thẩm quyền.

5. Bảo đảm các yêu cầu về an toàn thông tin theo quy định của Điều 11 Quy chế này;

Chương IV **TỔ CHỨC THỰC HIỆN**

Điều 16. Khen thưởng và xử lý vi phạm

1. Hàng năm, Phòng Văn hóa và Thông tin dựa trên các điều tra, báo cáo công tác an toàn, an ninh thông tin của các cơ quan, đơn vị để xác lập bảng xếp hạng an toàn, an ninh thông tin, trên cơ sở đó đề xuất UBND thị xã Từ Sơn xem xét khen thưởng theo quy định hiện hành.

2. Các cơ quan, đơn vị có hành vi vi phạm Quy chế này tùy theo tính chất, mức độ vi phạm mà bị xử lý theo quy định của pháp luật hiện hành.

Điều 17. Thủ trưởng các cơ quan, đơn vị trên địa bàn thị xã Từ Sơn chịu trách nhiệm tổ chức triển khai thực hiện Quy chế tại đơn vị mình.

Điều 18. Phòng Tài chính và Kế hoạch phối hợp Phòng Văn hóa và Thông tin ưu tiên bố trí kinh phí thực hiện các nhiệm vụ đảm bảo an toàn thông tin của thị xã.

Điều 19. Trong quá trình thực hiện, nếu có những vấn đề vướng mắc, đề nghị các cơ quan, đơn vị gửi về Phòng Văn hóa và Thông tin để tổng hợp, báo cáo UBND thị xã, Trưởng Ban Chỉ đạo xem xét, quyết định./.

TRƯỞNG BAN

CHỦ TỊCH UBND THỊ XÃ
Hoàng Bá Huy