UBND TỈNH NINH BÌNH
SỞ DU LỊCH

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

QUY CHẾ

Đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của Sở Du lịch tỉnh Ninh Bình

(Ban hành kèm theo Quyết định số: /QĐ-SDL ngày tháng 9 năm 2021 của Sở Du lịch tỉnh Ninh Bình)

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 Sở Du lịch tỉnh Ninh Bình.

2. Quy chế được áp dụng đối với các phòng, đơn vị, cán bộ, công chức, viên chức và người lao động của Sở Du lịch tỉnh Ninh Bình.

Điều 2. Mục đích, nguyên tắc đảm bảo an toàn 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 cơ quan.

2. Luật An ninh mạng số 24/2018/QH14 ngày 12 tháng 6 năm 2018 chính thức có hiệu lực từ ngày 01 tháng 01 năm 2019

3. Các hoạt động ứng dụng công nghệ thông tin phải thực hiện theo Quyết định số 15/2016/QĐ-UBND ngày 06/7/2016 của UBND tỉnh Ninh Bình về việc 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 thuộc phạm vi quản lý của tỉnh Ninh Bình.

Chương II

QUY ĐỊNH ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 3. Quản lý vận hành trong công tác đảm bảo an toàn, an ninh thông tin

1. Việc bật, tắt máy tính, máy in….phải thực hiện theo hướng dẫn sử dụng thiết bị, hạn chế tối đa việc tắt đột ngột thiết bị (nguồn điện) khi đang sử dụng.

2. Không được tự ý luân chuyển, di dời thiết bị CNTT trong đơn vị khi chưa được phép của lãnh đạo Sở hoặc đơn vị đồng ý.

3. Không tự ý cài đặt các chương trình phần mềm, lắp đặt thiết bị phần cứng không phục vụ cho công tác chuyên môn nghiệp vụ.

4. Không truy cập các trang web không rõ nguồn gốc, check địa chỉ Email, đường linhk kết nối lạ để tránh phát tán virut, phần mềm gián điệp vào hệ thống máy tính trong cơ quan.

5. Không tự ý cấu hình máy tính cá nhân địa chỉ IP, tên máy trạm, nhóm làm việc (workgroup), vùng làm việc (domain), vị trí thiết bị mạng (wifi, router), làm ảnh hưởng đến hệ thống mạng dùng chung của Sở.

6. Khi sử dụng thiết bị lưu trữ bên ngoài vào hệ thống máy tính trong cơ quan (USB, HDD BOX,…) các tệp đính kèm trên thư điện tử cần kiểm tra và quét virut.

7. Kết thúc ngày làm việc, yêu cầu người sử dụng phải thoát khỏi các chương trình đang hoạt động, tắt máy tính, máy in đúng theo quy trình.

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 là khu vực hạn chế tiếp cận. 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, virus

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, viên chức và người lao động 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 hiện 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. Phải lập kế hoạch và thực hiện sao lưu dữ liệu phù hợp với điều kiện, 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. 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 nội dung 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 nội dung 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, viên chức và người lao động 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. 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.

5. 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.

6. 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:

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 đơn vị;

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 cơ quan;

d) 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 phải kịp thời khắc phục và hạn chế thiệt hại, báo cáo bằng văn bản cho cơ quan cấp trên trực tiếp quản lý và Sở Thông tin và Truyền thông.

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

Điều 11. Các hành vi bị nghiêm cấm

1. Không được lợi dụng việc sử dụng mạng Internet nhằm mục đích: chống lại nhà nước Cộng hoà xã hội chủ nghĩa Việt Nam, gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, kích động bạo lực, dâm ô, đồi truỵ, tệ nạn xã hội, mê tín dị đoan, phá hoại thuần phong mỹ tục của dân tộc.

2. Không được đưa hoặc thu thập các thông tin xuyên tạc, vu khống, xúc phạm uy tín của cơ quan, danh dự nhân phẩm của cán bộ, công chức, viên chức, người lao động hoặc công dân khác.

3. Không được chơi các trò chơi trực tuyến (Game online) hoặc các trò chơi khác trên Internet trong giờ làm việc.

4. Tạo ra, cài đặt, phát tán vi rút máy tính, phần mềm độc hại trái pháp luật.

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

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

7. 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.

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

Chương III

TRÁCH NHIỆM ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 12. Trách nhiệm của các phòng, đơn vị trực thuộc Sở

1. Tuyên truyền, nâng cao nhận thức cho cán bộ công chức, viên chức về các nguy cơ mất an toàn, an ninh thông tin và các nội dung quy định tại Quy chế này.

2. Khi có sự cố hoặc nguy cơ mất an toàn thông tin phải kịp thời thông báo cho cán bộ phụ trách CNTT để báo cáo Giám đốc Sở và Sở Thông tin và Truyền thông khi cần thiết.

3. Hủy bỏ quyền truy cập vào hệ thống thông tin, thu hồi lại các tài liệu, hồ sơ, thông tin liên quan tới tài khoản của CBCCVC chuyển công tác, nghỉ hưu hoặc chấm dứt hợp đồng.

4. Thường xuyên tổ chức thực hiện tự kiểm tra, rà soát, phân tích, đánh giá, báo cáo rủi ro và nguy cơ gây mất an toàn, an ninh thông tin đối với hệ thống thông tin của đơn vị.

5. Phối hợp với Sở Thông tin và Truyền thông và các đơn vị có liên quan trong công tác xây dựng, bảo trì, nâng cấp hệ thống bảo đảm an toàn, an ninh thông tin của đơn vị.

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

Điều 13. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các cơ quan

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

a) Chịu trách nhiệm đảm bảo an toàn thông tin của đơn vị;

b) 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;

c) 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;

d) 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;

e) Thường xuyên cập nhật, nâng cao kiến thức, trình độ chuyên môn đáp ứng yêu cầu đảm bảo an toàn thông tin của đơn vị.

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

a) Nghiêm túc chấp hành các quy định của 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;

b) Mỗi cán bộ, công chức, viên chức và người lao động phải có trách nhiệm tự quản lý, bảo quản thiết bị được giao sử dụng;

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

d) Tham gia các chương trình đào tạo, tập huấn để nâng cao kiến thức, trình độ chuyên môn đáp ứng yêu cầu đảm bảo an toàn thông tin của cơ quan.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 14. Khen thưởng và xử lý vi phạm

1. Tập thể và cá nhân có thành tích xuất sắc trong công tác an toàn, an ninh thông tin của các phòng chuyên môn, đơn vị trực thuộc Sở được xem xét khen thưởng theo quy định hiện hành.

2. Các phòng chuyên môn, đơn vị trực thuộc Sở, cá nhân có hành vi vi phạm Quy chế này tùy theo tính chất, mức độ vi phạm sẽ bị xử lý theo quy định của pháp luật.

Điều 15. Triển khai tổ chức thực hiện Quy chế và sửa đổi, bổ sung Quy chế.

1. Văn phòng Sở có trách nhiệm chủ trì phối hợp với các phòng chuyên môn, đơn vị trực thuộc có liên quan hướng dẫn triển khai thực hiện Quy chế này.

2. Trong quá trình thực hiện Quy chế, nếu có vướng mắc, phát sinh, các phòng chuyên môn, đơn vị trực thuộc kịp thời phản ánh về Văn phòng Sở để tổng hợp, báo cáo Lãnh đạo Sở xem xét sửa đổi, bổ sung cho phù hợp./.

GIÁM ĐỐC

Bùi Văn Mạnh