UBND TỈNH HÀ NAM
SỞ VĂN HÓA, THỂ THAO VÀ DU LỊCH

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

Số:13 /QĐ-SVHTTDL

Hà Nam, ngày 18 tháng 01 năm 2021

QUYẾT ĐỊNH
Ban hành Quy chế Đảm bảo an toàn thông tin trên máy tính, mạng máy tính và các thiết bị công nghệ thông tin trong hoạt động của Sở Văn hóa, Thể thao và Du lịch

GIÁM ĐỐC SỞ VĂN HÓA, THỂ THAO VÀ DU LỊCH

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;

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

Căn cứ Pháp lệnh bảo vệ bí mật nhà nước số 30/2000/PL-UBTVQH10 ngày 28 tháng 12 năm 2000 của Ủy ban Thường vụ Quốc hội;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động cơ quan nhà nước.

Căn cứ Quyết định số 23/2017/QĐ-UBND ngày 28 tháng 7 năm 2017 của Uỷ ban nhân dân tỉnh Hà Nam về Ban hành Quy chế Đảm bảo an toàn thông tin trên máy tính, mạng máy tính và các thiết bị công nghệ thông tin trong hoạt động của các cơ quan nhà nước tỉnh Hà Nam.

Căn cứ Quyết định số 19/2016/QĐ-UBND ngày 08/7/2016 của UBND tỉnh Hà Nam về việc quy định chức năng, nhiệm vụ quyền hạn và cơ cấu tổ chức của Sở Văn hóa, Thể thao và Du lịch tỉnh Hà Nam

Xét đề nghị của Chánh Văn phòng Sở,

QUYẾT ĐỊNH:

Điều 1. Ban hành Quy chế đảm bảo an toàn thông tin trên máy tính, mạng máy tính và các thiết bị công nghệ thông tin trong hoạt động của Sở Văn hóa, Thể thao và Du lịch.

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

Điều 3. Chánh Văn phòng Sở Văn hóa, Thể thao và Du lịch, Thủ trưởng các đơn vị trực thuộc, công chức, viên chức và người lao động Sở Văn hóa, Thể thao và Du lịch chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Sở Thông tin và Truyền thông
- Ban Giám đốc Sở (để b/c);
- Thủ trưởng các phòng, đơn vị trực thuộc;
- Như Điều 3;
- Lưu: VT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XHCN VIỆT NAM
SỞ VĂN HÓA THỂ THAO VÀ DU LỊCH
TỈNH HÀ NAM

Tạ Đình Quyền

UBND TỈNH HÀ NAM
SỞ VĂN HÓA, THỂ THAO VÀ DU LỊCH

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

Hà Nam, ngày tháng năm 2021

QUY CHẾ
Đảm bảo an toàn thông tin trên máy tính, mạng máy tính và các thiết bị công nghệ thông tin trong hoạt động của Sở Văn hóa, Thể thao và Du lịch

(Ban hành kèm theo Quyết định số: /QĐ-SVHTTDL ngày tháng năm 2021 của Sở Văn hóa, Thể thao và Du lịch)

Chương I
NHỮNG QUY ĐỊNH CHUNG

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

1. Quy chế này quy định về đảm bảo an toàn thông tin (ATTT) trên máy tính, mạng máy tính và các thiết bị công nghệ thông tin (CNTT) trong hoạt động ứng dụng CNTT của Sở Văn hóa, Thể thao và Du lịch.

2. Quy chế này áp dụng đối với:

- Các phòng, đơn vị trực thuộc Sở Văn hóa, Thể thao và Du lịch (sau đây gọi tắt là cơ quan, đơn vị).

- Các tổ chức, cá nhân có tham gia quản lý, vận hành, khai thác và sử dụng các ứng dụng CNTT trong hoạt động của các cơ quan nhà nước tại Sở Văn hóa, Thể thao và Du lịch.

Điều 2. Các nguyên tắc chung về đảm bảo ATTT

1. Các hoạt động ứng dụng CNTT phải tuân theo nguyên tắc đảm bảo ATTT được quy định tại Điều 41 Nghị định 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng CNTT trong hoạt động cơ quan nhà nước.

2. Áp dụng Quy chế này nhằm giảm thiểu các nguy cơ gây mất ATTT trên máy tính, mạng máy tính và các thiết bị CNTT trong các cơ quan, đơn vị.

3. Xử lý sự cố ATTT trên máy tính, mạng máy tính và các thiết bị CNTT phải đảm bảo quyền lợi hợp pháp của các tổ chức, cá nhân, không xâm phạm đời sống riêng tư, bí mật cá nhân, thông tin của cơ quan, đơn vị.

4. Các tài liệu có nội dung thuộc danh mục bí mật nhà nước không được truyền trên mạng mà phải được quản lý theo chế độ mật đúng quy định của pháp luật hiện hành.

5. Nghiêm cấm việc sử dụng máy tính kết nối Internet, thiết bị lưu trữ di động, thiết bị di động thông minh để tạo lập, lưu giữ tài liệu có nội dung mật. Các thiết bị viễn thông, máy tính được sử dụng soạn thảo, lưu giữ tài liệu có nội dung mật phải được kiểm tra, chứng nhận của cơ quan chức năng trước khi đưa

vào sử dụng.

6. Các thiết bị viễn thông, máy tính có chứa tài liệu của cơ quan nhà nước khi đưa đi công tác nước ngoài phải thực hiện theo quy định của pháp luật về bảo vệ bí mật của nhà nước.

7. Tổ chức, cá nhân không được xâm phạm ATTT trên máy tính, mạng máy tính và các thiết bị CNTT của tổ chức, cá nhân khác.

8. Thủ trưởng các phòng, đơn vị phải có phương án tổ chức sao lưu dữ liệu dự phòng cho mọi dữ liệu quan trọng của tỉnh, của phòng, đơn vị và chịu trách nhiệm nếu để xảy ra mất mát dữ liệu do không tiến hành sao lưu dự phòng.

9. Để phục vụ hoạt động theo dõi, giám sát, phân tích và điều tra, các phòng đơn vị phải thực hiện việc lưu trữ nhật ký hoạt động của các hệ thống tại các máy chủ (hệ điều hành và các phần mềm ứng dụng) trong thời gian ít nhất là 30 ngày.

10. Hoạt động ATTT máy tính, mạng máy tính và các thiết bị CNTT phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.

Chương II
QUY ĐỊNH ĐẢM BẢO ATTT

Điều 3. Quản lý gửi thông tin

1. Việc gửi, nhận thông tin trên máy tính, mạng máy tính và các thiết bị CNTT phải đảm bảo các yêu cầu sau đây:

a) Không giả mạo nguồn gốc gửi thông tin.

b) Tuân thủ quy định của Luật ATTT mạng và các quy định khác của pháp luật có liên quan.

2. Các phòng, đơn vị phải sử dụng hộp thư điện tử công vụ với địa chỉ tên miền "hanam.gov.vn" được cấp phát để trao đổi thông tin, văn bản điện tử trong quá trình xử lý công việc. Không sử dụng các hộp thư khác như gmail, yahoo…vv.

3. Việc gửi văn bản qua hệ thống phần mềm Quản lý văn bản và điều hành; Một cửa điện tử và Dịch vụ công trực tuyến; các phần mềm chuyên ngành khác phải sử dụng loại văn bản đã có dấu, chữ ký được quét (scan) dưới dạng tệp tin định dạng *.PDF và ký số trước khi gửi.

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 có các biện pháp bảo vệ, ngăn chặn xâm nhập trái phép vào phòng máy chủ.

2. Phòng máy chủ của các phòng, đơn vị là khu vực hạn chế tiếp cận. Chỉ có người có trách nhiệm theo quy định của Thủ trưởng phòng, đơn vị mới được phép vào phòng máy chủ.

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

4. Cán bộ quản lý phòng máy chủ phải thường xuyên theo dõi, bảo đảm an toàn môi trường vật lý (nhiệt độ, độ ẩm, ánh sáng,…) cho phòng máy chủ, các hệ thống hỗ trợ như: máy điều hòa, nguồn điện, đường truyền cáp quang, hệ thống báo

cháy phải luôn trong tình trạng hoạt động tốt.

5. Thủ trưởng các phòng, đơn vị phải chỉ đạo các bộ phận chức năng có biện pháp bảo vệ đối với phòng máy chủ nhằm phòng, chống nguy cơ do cháy nổ, ngập lụt, động đất và các thảm họa khác do thiên nhiên và con người gây ra.

Điều 5. Phòng chống mã độc, Virus

1. Các hệ thống thông tin quan trọng như: Cổng Thông tin điện tử, thư điện tử, Quản lý văn bản và điều hành, Một cửa điện tử và Dịch vụ công trực tuyến… phải thường xuyên cập nhật phiên bản mới, bản vá lỗi, phần mềm nhằm kịp thời phát hiện, loại trừ các mã độc, Virus máy tính.

2. Tất cả các máy tính được trang bị và kết nối mạng tại các phòng, đơn vị phải được cài đặt, trang bị phần mềm diệt Virus có bản quyền và thiết lập chế độ tự động cập nhật các mẫu mã độc, Virus mới; chế độ tự động quét khi mở các tập tin.

3. Cán bộ, công chức, viên chức trong phòng, đơn vị phải được hướng dẫn về phòng chống mã độc, các rủi ro do mã độc, Virus gây ra.

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

5. Tất cả các máy tính của phòng, đơn vị phải được cấu hình nhằm vô hiệu hóa tính năng tự động thực thi (auto play) các tệp tin trên thiết bị lưu trữ di động.

6. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến bị nhiễm mã độc, Virus trên máy tính của phòng, đơn vị (máy chạy chậm bất thường, cảnh báo từ phần mềm chống mã độc, mất dữ liệu…) người sử dụng phải tắt máy và báo cho cán bộ có trách nhiệm của phòng, đơn vị để xử lý.

Điều 6. Sao lưu dữ liệu dự phòng

1. Các dữ liệu quan trọng của phòng, đơn vị 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 phòng, đơn vị phải lập kế hoạch và thực hiện sao lưu dữ liệu phù hợp với điều kiện từng phòng, đơn vị đảm bảo phục hồi dữ liệu ngay sau khi có sự cố xảy ra.

Điều 7. Quản lý thiết bị tường lửa

1. Hệ thống mạng máy tính của phòng, đơn vị phải được trang bị tường lửa để ngăn chặn và phát hiện các thâm nhập trái phép vào hệ thống mạng.

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

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

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

2. Nhật ký 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 được ghi nhật ký gồm: quá trình đăng nhập hệ thống; tạo, cập nhật, xóa dữ liệu; các hành vi xem, cấu hình hệ thống; thiết lập các kết nối vào, ra hệ thống; thay đổi quyền truy cập hệ thống.

4. Cán bộ chuyên trách CNTT của các phòng, đơn vị thường xuyên theo dõi bản ghi nhật ký 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 của phòng, đơn vị phải chi tiết và tổ chức thực hiện nghiêm túc, phù hợp với các quy định của pháp luật về ATTT.

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

3. Cán bộ, công chức, 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 khóa tài khoản trong một khoảng thời gian nhất định trước khi cho đăng nhập lại.

5. Tất cả các máy chủ, máy trạm phải được đặt mật khẩu truy cập và thiết lập chế độ tự khóa sau 1 thời gian nhất định không sử dụng.

6. Khi triển khai lắp đặt các thiết bị: router, switch, wifi… phải thiết lập mật khẩu mới thay cho mật khẩu mặc định của thiết bị.

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

8. Mật khẩu đăng nhập vào hệ thống thông tin phải đảm bảo độ phức tạp cao (có ít nhất 8 ký tự bao gồm ký tự thường, ký tự số và ký hiệu đặc biệt). Đối với hệ thống phần mềm mới đưa vào sử dụng phải tiến hành đổi mật khẩu người dùng ngay khi được cấp, tiếp nhận tài khoản. Định kỳ thay đổi mật khẩu (ít nhất 30 ngày đổi một lần), không đặt chế độ ghi nhớ mật khẩu khi sử dụng.

9. Cán bộ chuyên trách CNTT của các phòng, đơn vị phải thực hiện hủy tài khoản, quyền truy cập hệ thống các hệ thống thông tin, thu hồi lại tất cả các tài sản liên quan đến hệ thống thông tin (khóa, thẻ nhận dạng, thư mục lưu trữ, thư điện tử, chữ ký số, máy vi tính…) đối với các cá nhân nghỉ việc, chuyển công tác.

Điều 10. Quản lý thiết bị

1. Thiết bị CNTT đặt tại phòng máy chủ của các phòng, đơn vị phải đặt tên và dán nhãn đúng quy định.

2. Khi sửa chữa các thiết bị CNTT, hạn chế cho phép mang thiết bị, nhất là thiết bị lưu trữ dữ liệu ra khỏi phòng, đơn vị và bố trí cán bộ giám sát.

3. Khi thanh lý tài sản là thiết bị CNTT có lưu trữ dữ liệu, phải xóa dữ liệu để không thể phục hồi nhằm đảm bảo bí mật các dữ liệu có trên các thiết bị đó.

Điều 11. Quản lý bản quyền phần mềm

1. Các phần mềm, chương trình ứng dụng sử dụng cho máy chủ tại các phòng, đơn vị nếu là phần mềm mã nguồn đóng thì phải có bản quyền sử dụng theo đúng quy định của pháp luật. Khuyến khích sử dụng các phần mềm mã nguồn mở.

2. Cán bộ, công chức, viên chức và người lao động trong các phòng, đơn vị không phát tán chia sẻ phần mềm có bản quyền đã được đầu tư, cấp phát cho các đối tượng ngoài phòng, đơn vị với mục đích ngoài nhiệm vụ chuyên môn được giao.

Điều 12. An toàn cho máy tính cá nhân (máy tính để bàn, máy tính xách tay)

1. Cài đặt phần mềm diệt Virus, mã độc cho tất cả các máy tính trong mạng LAN của phòng, đơn vị. Thiết lập chế độ cập nhật hàng ngày cho phần mềm diệt Virus, mã độc.

2. Thủ trưởng các phòng, đơn vị phải quán triệt cán bộ, công chức, viên chức không được cài đặt phần mềm không rõ nguồn gốc, xuất xứ; không truy cập các trang web có nội dung không lành mạnh; không mở những thư điện tử không rõ địa chỉ người gửi… nhằm tránh tối đa việc phần mềm Virus, mã độc tự động cài đặt vào máy tính cá nhân.

3. Mã hóa phân vùng ổ cứng chứa dữ liệu quan trọng trên các máy tính cá nhân; đặt mật khẩu mở các tệp tài liệu khi gửi trên môi trường mạng trong các trường hợp cần thiết.

4. Không chia sẻ thư mục trên mạng LAN theo cơ chế cho phép toàn quyền đọc, ghi (Share Full), chỉ thiết lập cơ chế chỉ đọc (Read Only) và yêu cầu sử dụng mật khẩu khi truy cập thư mục chia sẻ.

Điều 13. An toàn khi sử dụng các thiết bị lưu trữ ngoài

1. Việc sử dụng các thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB,… phải quét Virus, mã độc trước khi đọc hoặc sao chép dữ liệu.

2. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu.

Điều 14. Soạn thảo nội dung thuộc bí mật nhà nước

1. Thủ trưởng phòng, đơn vị phải nghiên cứu, xác định độ mật của các văn bản có nội dung thuộc danh mục bí mật nhà nước do phòng, đơn vị, địa phương ban hành để quản lý theo đúng quy định.

2. Đảm bảo an toàn khi sử dụng máy tính cho soạn thảo văn bản có nội dung thuộc bí mật nhà nước, các phòng đơn vị cần bố trí 01 máy tính dùng riêng có đặt mật khẩu bảo vệ và không kết nối với mạng LAN, Internet theo đúng quy định về soạn thảo các văn bản có tính chất Mật.

Điều 15. 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 phòng, đơn vị.

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

d) Khẩn cấp: sự cố ảnh hưởng đến hoạt động của nhiều hoạt động chính của phòng, đơn vị.

2. Khi có sự cố hay nguy cơ gây mất ATTT, Thủ trưởng phòng, đơn vị phải chỉ đạo kịp thời để khắc phục và hạn chế các thiệt hại, báo cáo nhanh qua điện thoại, thư điện tử và bằng văn bản cho đơn vị chuyên trách CNTT, Sở Thông tin và Truyền thông.

3. Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp vượt quá khả năng khắc phục của phòng, đơn vị, thủ trưởng phòng, đơn vị phải báo cáo ngay cho Sở Thông tin và Truyền thông để có phương án hỗ trợ, khắc phục.

Chương III
TRÁCH NHIỆM ĐẢM BẢO ATTT

Điều 16. Trách nhiệm của Văn phòng Sở

1. Tham mưu với Lãnh đạo Sở về công tác đảm bảo ATTT trong Sở Văn hóa, Thể thao và Du lịch và chịu trách nhiệm trước Lãnh đạo Sở trong việc đảm bảo an toàn cho các hệ thống thông tin dùng chung của Sở như: Cổng Thông tin điện tử, thư điện tử, Quản lý văn bản và Điều hành.

2. Chịu trách nhiệm xây dựng và trình Lãnh đạo Sở ban hành các cơ chế, chính sách và hướng dẫn, khuyến nghị về đảm bảo ATTT cho các phòng, đơn vị.

3. Tham mưu với Lãnh đạo Sở hướng dẫn việc sử dụng các thiết bị CNTT để lưu giữ và truyền tải thông tin bí mật nhà nước.

4. Thông báo cho các phòng, đơn vị biết và có biện pháp phòng ngừa, ngăn chặn rủi ro, các nguy cơ mất ATTT do Virus, phần mềm độc hại, phần mềm gián điệp gây ra.

5. Định kỳ 6 tháng, hàng năm, hoặc đột xuất tổng hợp báo cáo Lãnh đạo Sở về tình hình đảm bảo ATTT trong Sở Văn hóa, Thể thao và Du lịch.

Điều 17. Trách nhiệm của các phòng, đơn vị

1. Thủ trưởng các phòng, đơn vị có trách nhiệm tổ chức quán triệt, nâng cao nhận thức cho cán bộ, công chức, viên chức về đảm bảo ATTT; tổ chức triển khai thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước Lãnh đạo Sở trong công tác đảm bảo ATTT của phòng, đơn vị mình.

2. Bảo vệ ATTT trong mạng nội bộ là trách nhiệm của các phòng, đơn vị quản lý mạng nội bộ đó.

3. Trang bị đầy đủ kiến thức bảo mật cơ bản cho cán bộ, công chức, viên chức về ATTT trước khi cho phép truy nhập và sử dụng Hệ thống thông tin. Bố trí, tạo điều kiện làm việc phù hợp với chuyên môn và ưu tiên bồi dưỡng nghiệp vụ về ATTT cho cán bộ chuyên trách (hoặc cán bộ được giao phụ trách) về CNTT trong các phòng, đơn vị. Khuyến khích các phòng, đơn vị liên kết với tổ chức, cá nhân, doanh nghiệp CNTT uy tín mở các khóa đào tạo nhân lực trong lĩnh vực ATTT.

4. Bố trí kinh phí cho việc mua sắm, nâng cấp các trang thiết bị phần cứng, phần mềm để đảm bảo và tăng cường ATTT trong hoạt động ứng dụng CNTT của phòng, đơn vị.

5. Khi có sự cố ATTT hoặc có nguy cơ mất ATTT phải kịp thời chỉ đạo khắc phục ngay, ưu tiên sử dụng cán bộ kỹ thuật chuyên trách trong phòng, đơn vị. Kịp thời báo cho doanh nghiệp cung cấp dịch vụ và thông báo bằng văn bản cho Văn phòng Sở, Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ xử lý.

6. Phối hợp với Văn phòng Sở Văn hóa, Thể thao và Du lịch, Sở Thông tin và Truyền thông và các phòng, đơn vị liên quan thực hiện công tác kiểm tra khắc phục sự cố ATTT; đồng thời cung cấp đầy đủ các thông tin khi đoàn kiểm tra yêu cầu. Không được che giấu thông tin về sự cố nhằm gây khó khăn cho các cơ quan chức năng đánh giá thiệt hại để có phương án xử lý.

Điều 18. Trách nhiệm các tổ chức, cá nhân tham gia quản lý, vận hành, khai thác ứng dụng CNTT trong cơ quan nhà nước

1. Tuân thủ theo quy định tại Quy chế này và các quy định khác của pháp luật có liên quan.

2. Thực hiện tốt các biện pháp đảm bảo ATTT khi tương tác, sử dụng ứng dụng CNTT của các cơ quan nhà nước phục vụ người dân và doanh nghiệp.

3. Chịu trách nhiệm về các thông tin cá nhân đăng ký, khai báo khi sử dụng tương tác các ứng dụng CNTT của tỉnh; tuân thủ các hướng dẫn khi sử dụng dịch vụ CNTT của tỉnh.

4. Không thu thập, sử dụng, phát tán, quảng cáo, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống dịch vụ ứng dụng CNTT thông tin để thu thập, khai thác thông tin cá nhân.

Điều 19. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong phòng, đơn vị

1. Trách nhiệm của cán bộ chuyên trách hoặc cán bộ được giao phụ trách CNTT trong phòng, đơn vị:

- Chịu trách nhiệm đảm bảo ATTT của phòng, đơn vị.

- Chịu trách nhiệm triển khai các biện pháp quản lý, vận hành, quản lý kỹ thuật, tham mưu xây dựng quy định về đảm bảo an toàn cho hệ thống thông tin của phòng, đơn vị mình theo quy chế này.

- Thực hiện việc giám sát, đánh giá, báo cáo thủ trưởng phòng, đơn vị các rủi ro mất ATTT và mức độ nghiêm trọng của các rủi ro đó.

- Phối hợp với các cá nhân, các phòng, đơn vị có liên quan trong việc kiểm tra, phát hiện và khắc phục các sự cố mất ATTT.

2. Trách nhiệm của cán bộ, công chức, viên chức và người lao động

- Chấp hành nghiêm túc các quy định về ATTT của các phòng, đơn vị cũng như các quy định khác của pháp luật, nâng cao ý thức cảnh giác và trách nhiệm đảm bảo ATTT tại phòng, đơn vị.

- Khi phát hiện sự cố mất ATTT phải báo ngay với cấp trên và bộ phận chuyên trách của phòng, đơn vị để kịp thời ngăn chặn, xử lý. Không tự ý liên hệ với cá nhân bên ngoài vào can thiệp các thiết bị phần cứng, phần mềm của phòng, đơn vị mình.

- Không sử dụng hòm thư công vụ có địa chỉ tên miền “hanam.gov.vn”

được cấp phát cho cá nhân hoặc phòng, đơn vị mình vào mục đích cá nhân như đăng ký tài khoản mạng xã hội, đăng ký mua sắm qua mạng.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 20. Khen thưởng và xử lý vi phạm

1. Hàng năm, Sở Văn hóa, Thể thao và Du lịch dựa trên các điều tra, báo cáo công tác ATTT của các phòng, đơn vị tham mưu với Lãnh đạo Sở đưa ATTT vào tiêu chí đánh giá thi đua của các phòng, đơn vị.

2. Các phòng, đơn vị, tổ chức, cá nhân 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 21. Điều khoản thi hành

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

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Tạ Đình Quyền