UBND TỈNH THANH HÓA
SỞ VĂN HÓA, THỂ THAO
VÀ DU LỊCH

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

Dự Thảo

QUY CHẾ
Bảo đảm an toàn, an ninh thông tin trong lĩnh vực ứng dụng công nghệ thông tin của Sở Văn hóa, Thể thao và Du lịch Thanh Hóa

(Ban hành kèm theo Quyết định số: /QĐ-VHTTDL ngày tháng năm 2012 của Văn hóa, Thể thao và Du lịch Thanh Hóa)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về nội dung, biện pháp bảo đảm an toàn, an ninh thông tin trong lĩnh vực ứng dụng công nghệ thông tin (sau đây gọi tắt là CNTT) phục vụ cho công tác điều hành và quản lý hành chính nhà nước của Sở Văn hóa, Thể thao và Du lịch Thanh Hóa.

Điều 2. Đối tượng áp dụng

Quy chế này được áp dụng với tất cả các phòng, ban và các đơn vị sự nghiệp thuộc Sở Văn hóa, Thể thao và Du lịch Thanh Hóa.

Điều 3. Giải thích từ ngữ

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

1. Cán bộ chuyên trách CNTT (CBCT CNTT): Là cán bộ kỹ thuật hoặc cán bộ quản lý có chuyên môn về lĩnh vực CNTT, trực tiếp tham mưu cho lãnh đạo khai thác, quản lý và thực hiện công tác ứng dụng CNTT tại cơ quan, đơn vị, bảo đảm kỹ thuật và an toàn, an ninh thông tin cho việc khai thác, vận hành hệ thống CNTT tại đơn vị.

2. Tính tin cậy: bảo đảm thông tin chỉ có thể được truy cập bởi những người được cấp quyền sử dụng.

3. Tính toàn vẹn: bảo vệ sự chính xác và đầy đủ của thông tin và các phương pháp xử lý.

4. Tính sẵn sàng: bảo đảm những người được cấp quyền có thể truy cập thông tin và các tài sản liên quan ngay khi có nhu cầu.

5. An toàn, an ninh thông tin (ATANTT): bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin đối với nguy cơ tự nhiên hoặc do con người gây ra. Việc bảo vệ thông tin, tài sản và con người trong hệ thống thông tin nhằm bảo đảm cho các hệ thống thực hiện đúng chức năng, phục vụ đúng đối tượng, tính sẵn sàng cao với yêu cầu chính xác và tin cậy. An toàn, an ninh thông tin bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu của máy tính và an toàn mạng.

6. TCVN 7562:2005: Tiêu chuẩn Việt Nam về mã thực hành quán lý an toàn thông tin.

7. ISO 17799:2005: Tiêu chuẩn quốc tế cung cấp các hướng dẫn quản lv an toàn, bảo mật thông tin dựa trên những quy phạm công nghiệp tốt nhất (tập quy phạm cho quản lý an toàn bảo mật thông tin).

8. ISO 27001:2005: tiêu chuẩn quốc tế về quản lý bảo mật thông tin do Tổ chức Chất lượng Quốc tế và Hội đồng Điện tử Quốc tế xuất bản vào tháng 10/2005.

Chương II
NỘI DUNG BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN

Điều 4. Các biện pháp quản lý kỹ thuật cơ bản cho công tác an toàn, an ninh thông tin.

1. Tổ chức mô hình mạng: Cài đặt, cấu hình, tổ chức hệ thống mạng theo mô hình Clients/Server, hạn chế sử dụng mô hình mạng ngang hàng. Khi thiết lập các dịch vụ trên môi trường mạng Internet, chỉ cung cấp những chức năng thiết yếu nhất bảo đảm duy trì hoạt động của hệ thống thông tin; hạn chế sử dụng chức năng, cổng giao tiếp mạng, giao thức và các dịch vụ không cần thiết.

2. Quản lý hệ thống mạng không dây: định kỳ 3 tháng thay đổi mật khẩu nhằm tăng cường công tác bảo mật.

3. Tổ chức quản lý tài khoản: Các tài khoản và định danh người dùng trong hệ thống thông tin, bao gồm: tạo mới, kích hoạt, sửa đổi và loại bỏ các tài khoản, đồng thời tổ chức kiểm tra các tài khoản của hệ thống thông tin ít nhất 6 tháng 1 lần thông qua các công cụ của hệ thống. Hủy tài khoản, quyền truy nhập hệ thống thông tin, thu hồi lại tất cả các tài sản liên quan tới hệ thống thông tin (khóa, thẻ nhận dạng, thư mục lưu trữ,...) đối với cán bộ, công chức, viên chức đã chuyển công tác, chấm dứt hợp đồng lao động.

4. Quản lý đăng nhập hệ thống: Các hệ thống thông tin cần giới hạn số lần đăng nhập vào hệ thống. Hệ thống tự động khóa tài khoản hoặc cô lập tài khoản khi liên tục đăng nhập sai vượt quá số lần quy định. Tổ chức theo dõi, giám sát tất cả các phương pháp đăng nhập từ xa (quay số, internet,...), nhất là các đăng nhập có chức năng quản trị, tăng cường việc sử dụng mạng riêng ảo (VPN - Virtual Private Network) khi có nhu cầu làm việc từ xa; yêu cầu người sử dụng đặt mật khẩu với độ an toàn cao, giám sát, nhắc nhở khuyến cáo nên thay đổi thường xuyên mật khẩu.

5. Quản lý Logfile: Hệ thống thông tin cần ghi nhận các sự kiện: quá trình đăng nhập vào hệ thống, các thao tác cấu hình hệ thống. Thường xuyên kiểm tra, sao lưu (backup) các logfile theo từng tháng để lưu vết theo dõi, xác định những sự kiện đã xảy ra của hệ thống và hạn chế việc tràn logfile gây ảnh hưởng đến hoạt động của hệ thống.

6. Chống mã độc, virus: Lựa chọn, triển khai các phần mềm chống virus, thư rác trên các máy chủ, các thiết bị di động trong mạng và những hệ thống thông tin xung yếu như: cổng thông tin điện tử, thư điện tử, một cửa điện tử,... để phát hiện, loại trừ những đoạn mã độc hại (Virus, trojan, worms,...) và hỗ trợ người sử dụng cài đặt các phần mềm này trên máy trạm. Thường xuyên cập nhật các phiên bản (Version) mới, các bản vá lỗi của các phần mềm chống virus để bảo đảm chương trình quét virus của cơ quan trên các máy chủ, máy trạm luôn được cập nhật mới nhất, thiết lập chế độ quét thường xuyên ít nhất là hằng tuần.

7. Tổ chức quản lý tài nguyên: Kiểm tra, giám sát chức năng chia sẻ thông tin (Network File and Folder Sharing). Tổ chức cấp phát tài nguyên trên máy chủ theo danh mục thư mục cho từng phòng/đơn vị trực thuộc; khuyến cáo người sử dụng cân nhắc việc chia sẻ tài nguyên cục bộ trên máy đang sử dụng, tuyệt đối không được chia sẻ toàn bộ ổ cứng. Khi thực hiện việc chia sẻ tài nguyên trên máy chủ hoặc trên máy cục bộ nên sử dụng mật khẩu để bảo vệ thông tin.

8. Các biện pháp kỹ thuật bảo đảm an toàn cho Trang thông tin điện tử/ Cổng thông tin điện tử (gọi tắt là trang web):

a) Xác định cấu trúc thiết kế trang web: Quản lý toàn bộ các phiên bản của mã nguồn, phối hợp với đơn vị thực hiện dịch vụ hosting tổ chức mô hình trang web hợp lý tránh khả năng tấn công leo thang đặc quyền. Yêu cầu đơn vị cung cấp dịch vụ hosting phải cài đặt các hệ thống phòng vệ như tường lửa (firewall), thiết bị phát hiện/phòng chống xâm nhập (IDS/IPS) ở mức ứng dụng web (WAF- Web Application Firewall).

b) Vận hành ứng dụng web an toàn: Các trang web khi đưa vào sử dụng hoặc khi bổ sung thêm các chức năng, dịch vụ công mới cần liên hệ với Trung tâm ứng cứu khẩn cấp Máy tính Việt Nam (VNCERT) chi nhánh tại Hà Nội hoặc liên hệ với các tổ chức an ninh mạng đánh giá kiểm định nhằm tránh được các lỗi bảo mật thường xảy ra trên ứng dụng web.

c) Thiết lập và cấu hình cơ sở dữ liệu an toàn:

- Luôn cập nhật bản vá lỗi mới nhất cho hệ quản trị cơ sở dữ liệu; sử dụng công cụ để đánh giá, tìm kiếm lỗ hổng trên máy chủ cơ sở dữ liệu;

- Gỡ bỏ các cơ sở dữ liệu không sử dụng;

- Có các cơ chế sao lưu dữ liệu, tài liệu hóa quá trình thay đổi cấu trúc bằng cách xây dựng nhật ký CSDL với các nội dung như: nội dung thay đổi, lý do thay đổi, thời gian, vị trí thay đổi,...

d) Phối hợp với các nhà cung cấp dịch vụ hosting xây dựng phương án phục hồi trang web, trong đó chú ý mỗi tháng thực hiện việc backup toàn bộ nội dung trang web 1 lần bao gồm mã nguồn, cơ sở dữ liệu, dữ liệu phi cấu trúc,... để bảo đảm khi có sự cố có thể khắc phục lại ngay trong vòng 24 giờ.

9. Thiết lập cơ chế sao lưu và phục hồi máy chủ, máy trạm:

10. Xử lý khẩn cấp: Khi phát hiện hệ thống bị tấn công, thông qua các dấu hiệu như luồng, tin (traffic) tăng lên bất ngờ, nội dung trang chủ bị thay đổi, hệ thống hoạt động rất chậm khác thường,... cần thực hiện các bước cơ bản sau:

a) Bước 1 : Ngắt kết nối máy chủ ra khỏi mạng.

b) Bước 2: Sao chép logfile và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ (phục vụ cho công tác phân tích).

c) Bước 3: Khôi phục hệ thống bằng cách chuyển dữ liệu backup mới nhất để hệ thống hoạt động..

d) Bước 4: Thực hiện các công việc của khoản 2 Điều 8.

Điều 5. Các biện pháp quản lý vận hành trong công tác an toàn, an ninh thông tin

1. Đối với các cơ quan, đơn vị:

a) Phổ biến, hướng dẫn thực hiện các quy chế chung liên quan đến công tác ứng dụng CNTT đã được UBND tỉnh Thanh Hóa ban hành.

b) Kiểm tra việc thực hiện các nội dung của Điều 4 Quy chế này.

c) Tổ chức đào tạo tại đơn vị hoặc cử cán bộ tham gia các lớp đào tạo để trang bị các kiến thức về an toàn thông tin cơ bản cho cán bộ, công chức, viên chức trước khi cho phép truy nhập, vận hành, khai thác và sử dụng hệ thống thông tin.

d) Xác định và phân bố kinh phí chi thường xuyên cần thiết cho các hoạt động liên quan đến việc bảo vệ hệ thống thông tin, thông qua việc đầu tư các thiết bị tường lửa, các chương trình chống Spam, Virus trên các máy trạm, máy chủ,...

2. Đối với cán bộ chuyên trách CNTT:

a) Triển khai, thực hiện các nội dung của Điều 4 Quy chế này.

b) Tham mưu chuyên môn và vận hành an toàn hệ thống thông tin của đơn vị, triển khai các biện pháp bảo đảm an toàn, an ninh thông tin cho tất cả cán bộ, công chức, viên chức trong đơn vị mình.

c) Nắm vững và thực hiện nghiêm túc Pháp lệnh bảo vệ bí mật Nhà Nước ngày 28/12/2008. Thường xuyên tự cập nhật các kiến thức về an toàn, an ninh thông tin, nguy cơ tiềm ẩn có thể gây mất mát thông tin và các biện pháp phòng tránh khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ.

d) Thực hiện việc đánh giá, báo cáo các rủi ro và mức độ nghiêm trọng của các rủi ro đó. Các rủi ro đó có thể xảy ra do sự truy cập trái phép, sử dụng trái phép, mất, thay đổi hoặc phá hủy thông tin và hệ thống thông tin.

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

3. Đối với cán bộ, công chức, viên chức:

a) Thường xuyên cập nhật những chính sách, thủ tục an toàn thông tin của đơn vị cũng như thực hiện những hướng dẫn về an toàn, an ninh thông tin của cán bộ chuyên trách như một phần của công việc.

b) Hạn chế việc sử dụng chức năng chia sẻ tài nguyên (sharing), khi sử dụng chức năng này cần bật thuộc tính bảo mật bằng mật khẩu và thực hiện việc thu hồi chức năng này khi đã sử dụng xong.

c) Các máy tính khi không sử dụng trong thời gian dài (quá 2 giờ làm việc) cần tắt máy hoặc ngưng kết nối mạng, để tránh bị các hacker lợi dụng, sử dụng chức năng điều khiển từ xa dùng máy tính của mình tấn công vào các hệ thống thông tin khác.

d) Sử dụng chức năng mã hóa ở mức hệ điều hành bảo đảm các dữ liệu nhạy cảm như tài khoản, mật khẩu, các tập tin văn bản,... được mã hóa trước khi truyền trên môi trường mạng. Các tập tin gửi đính kèm bởi thư điện tử hoặc được tải xuống từ Internet hay các thiết bị lưu trữ gắn vào hệ thống cần được kiểm tra để phòng chống lây nhiễm virus hoặc phần mềm gián điệp gây mất mát thông tin.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 6. Trách nhiệm của Lãnh đạo đơn vị

1.Thủ trưởng các cơ quan, đơn vị có trách nhiệm thực hiện Điều 6 và Điều 7 của quy chế này và chịu trách nhiệm toàn diện trước Lãnh đạo tỉnh trong công tác bảo vệ an toàn hệ thống thông tin của đơn vị.

2. Khi có sự cố hoặc nguy cơ mất an toàn thông tin, kịp thời áp dụng mọi biện pháp để khắc phục và hạn chế thiệt hại; ưu tiên sử dụng lực lượng kỹ thuật an ninh thông tin của đơn vị và lập biên bản báo cáo bằng văn bản cho cơ quan Sở Văn hóa, Thể thao và Du lịch và Sở Thông tin và Truyền thông Thanh Hóa theo biểu mẫu tại Phụ lục 3 của Quy chế này.

Trường hợp có sự cố nghiêm trọng vượt quá khả năng khắc phục của đơn vị, phải báo cáo ngay cho Sở Văn hóa, Thể thao và Du lịch và Sở Thông tin và Truyền thông để Thanh Hóa cùng phối hợp xử lý.

3. Tạo điều kiện thuận lợi cho các cơ quan chức năng tham gia khắc phục sự cố và thực hiện đúng theo hướng dẫn.

4. Phối hợp với Đoàn kiểm tra để triển khai công tác kiểm tra, khắc phục sự cố được nhanh chóng và đạt hiệu quả; đồng thời cung cấp đầy đủ các thông tin khi Đoàn kiểm tra yêu cầu xuất trình.

5. Định kỳ hằng Quý, lập báo cáo tình hình an toàn, an ninh thông tin theo biểu mẫu tại Phụ lục 4 của Quy chế này và gửi về Sở Văn hóa, Thể thao và

Du lịch Thanh Hóa qua hộp thư điện tử svhttdl@thanhhoa.gov.vn . Riêng báo cáo thuộc quý IV của năm yêu cầu các đơn vị gửi bằng văn bản.

Điều 7. Trách nhiệm của cán bộ công chức trong các cơ quan, đơn vị quản lý hành chính nhà nước

1. Nghiêm chỉnh chấp hành các quy chế nội bộ, quy trình về an toàn, an ninh thông tin của Sở cũng như quy định khác của pháp luật, nâng cao ý thức cảnh giác và trách nhiệm bảo đảm an toàn, an ninh thông tin tại đơn vị

2. Khi phát hiện sự cố phải báo ngay với cơ quan cấp trên và bộ phận chuyên trách CNTT để kịp thời ngăn chặn, xử lý.

3. Hưởng ứng, tham gia các chương trình đào tạo, hội nghị về an toàn, an ninh thông tin do các cấp tổ chức.

Chương V
KHEN THƯỞNG, XỬ LÝ VI PHẠM

Điều 8. Khen thưởng

Các phòng, ban, đơn vị trực thuộc; cán bộ, công chức, viên chức và người lao động thực hiện tốt Quy chế này đem lại hiệu quả thiết thực sẽ được xem xét đánh giá khen thưởng.

Điều 9. Xử lý vi phạm

Các phòng, ban, đơn vị trực thuộc; cán bộ, công chức, viên chức và người lao động có hành vi vi phạm quy chế này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật theo trách nhiệm, xử phạt hành chính hoặc bị truy cứu trách nhiệm hình sự. Nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật hiện hành.

Chương VI
ĐIỀU KHOẢN THI HÀNH

Điều 10. Văn phòng, các phòng ban và đơn vị có liên quan triển khai thực hiện Quy chế này.

Trong quá trình thực hiện nếu có phát sinh khó khăn, vướng mắc cần sửa đổi, bổ sung các phòng ban, đơn vị kịp thời báo cáo về Văn phòng Sở tổng hợp trình Lãnh đạo sở xem xét, giải quyết.

Nơi nhận:
- BCĐ CCHC tỉnh (BC);
- Các đ/c lãnh đạo Sở;
- Trưởng cać phòng, ban, đơn vị liên quan;
- Bộ phận một cửa;
- Lưu: VP, VT.

GIÁM ĐỐC

Nguyễn Văn Tuấn