UỶ BAN NHÂN DÂN **TỈNH THÁI NGUYÊN**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 31/2013/QĐ-UBND	*Thái Nguyên, ngày 16 tháng 12 năm 2013*

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 tỉnh Thái Nguyên

ỦY BAN NHÂN DÂN TỈNH THÁI NGUYÊN

Căn cứ Luật Tổ chức Hội đồng nhân dân và Uỷ ban nhân dân ngày 26 tháng 11 năm 2003;

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 06 năm 2006;

Căn cứ Luật Giao dịch điện tử ngày 29 tháng 11 năm 2005;

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

Căn cứ Nghị định số 26/2007/NĐ-CP ngày 15 tháng 02 năm 2007 của Chính phủ Quy định chi tiết thi hành Luật Giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số;

Thực hiện Quyết định số 63/QĐ-TTg, ngày 13 tháng 01 năm 2010 của Thủ tướng Chính phủ về việc Phê duyệt Quy hoạch phát triển an toàn thông tin số quốc gia đến năm 2020;

Xét đề nghị của Sở Thông tin và Truyền thông tại Tờ trình số 699/TTr-STTTT ngày 13 tháng 11 năm 2013 và ý kiến thẩm định của Sở Tư pháp tại Văn bản số 500/STP-XDVB ngày 12 tháng 11 năm 2013,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn, an ninh thông tin trong lĩnh vực ứng dụng công nghệ thông tin của các cơ quan nhà nước thuộc tỉnh Thái Nguyên.

Điều 2. Quyết định này có hiệu lực thi hành sau 10 ngày kể từ ngày ký.

Điều 3. Chánh Văn phòng Uỷ ban nhân dân tỉnh; Giám đốc các sở, ban, ngành; Chủ tịch UBND các huyện, thành phố, thị xã và Thủ trưởng các cơ quan, tổ chức, cá nhân liên quan chịu trách nhiệm thi hành Quyết định này./.

TM. ỦY BAN NHÂN DÂN TỈNH
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

(Đã ký)

Nhữ Văn Tâm

UỶ BAN NHÂN DÂN **TỈNH THÁI NGUYÊN**	**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 các cơ quan nhà nước trên địa bàn tỉnh Thái Nguyên

(Ban hành kèm theo Quyết định số: 31/2013/QĐ/UBND ngày 16 tháng 12 năm 2013 của Uỷ ban nhân dân tỉnh Thái Nguyên)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về nội dung, biện pháp đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin phục vụ cho công tác điều hành và quản lý nhà nước trên địa bàn tỉnh Thái Nguyên.

Điều 2. Đối tượng áp dụng

Quy chế này được áp dụng đối với tất cả các cơ quan nhà nước trên địa bàn tỉnh Thái Nguyên (kể cả các cơ quan Trung ương đặt tại địa bàn tỉnh Thái Nguyên).

Điều 3. Giải thích từ ngữ

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

1. Cán bộ chuyên trách Công nghệ thông tin (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 quản lý an toàn thông tin.

7. ISO 17799:2005: Tiêu chuẩn quốc tế cung cấp các hướng dẫn quản lý 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.

9. Các từ tiếng Anh, từ kỹ thuật, từ chuyên ngành, từ được giải thích, ghi chú tại Phụ lục 2 của Quy chế này.

Chương II
NỘI DUNG ĐẢM BẢO 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. Đối với các sở, ngành, huyện, thành phố, thị xã có nhiều phòng, ban, đơn vị trực thuộc không nằm trong cùng một khu vực thì cần thiết lập mạng riêng ảo (VPN – Virtual Private Network) để tăng cường an ninh cho hạ tầng mạng nội bộ. 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 : Khi thiết lập mạng không dây để kết nối với mạng cục bộ thông qua các điểm truy nhập (Access Point -AP), cần thiết lập các tham số như: tên, SSID, mật khẩu, mã hóa dữ liệu và thông báo các thông tin liên quan đến AP để cơ quan sử dụng, 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, nhân viên 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 VPN 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, vi rút máy tính: Lựa chọn, triển khai các phần mềm chống vi rút máy tính, 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 (Vi rút máy tính, 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 vi rút máy tính để bảo đảm chương trình quét vi rút máy tính 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/ban; 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 đảm bảo 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 Công nghệ thông tin và Truyền thông Thái Nguyên 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 như: SQL Injection, Cross-Site Scripting (xss), Broken Authentication and Session Management, Insecure Direct Object References, Cross Site Request Forgery (CSRF), Security Misconfiguration, Failure to Restrict URL Access, Insecure Cryptographic Storage, Insufficient Transport Layer Protection, Unvalidated Redirects and Forwards...;

c) Thiết lập và cấu hình cơ sở dữ liệu (CSDL) 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:

a) Đối với máy trạm, máy chủ: Thực hiện việc sao lưu dữ liệu như hệ điều hành, các phần mềm ứng dụng văn phòng, phần mềm chuyên ngành...bằng các phần mềm như Pqmagic, FinalData, Symantec Ghost, ZAR (Zero Assumption Recovery), NovaBackup Professional, Nero BackItUp & Burn, Digital Rescue Premium...Sau

khi sao lưu mỗi máy được lưu vào các thiết bị lưu trữ như CD, ổ cứng ngoài...và thực hiện việc đánh số, dán nhãn để tránh nhầm lẫn nhằm phục vụ cho công tác phục hồi dữ liệu một cách nhanh nhất;

b) Đối với máy chủ: Cài đặt các dịch vụ Mirror, Raid, Clustering bảo đảm thiết lập cơ chế sao lưu và phục hồi hệ thống của máy chủ. Đối với các máy chủ cài đặt hệ điều hành Windows sử dụng chức năng System Restore để có thể dễ dàng khôi phục lại toàn bộ máy chủ hoặc các tập tin, thư mục được lựa chọn phục hồi.

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 Ủy ban nhân dân (UBND) tỉnh ban hành như Quy chế quản lý, vận hành và sử dụng hệ thống thư điện tử dùng chung tỉnh Thái Nguyên (*theo Quyết định số 957/QĐ-UBND ngày 22/5/2013 của Ủy ban nhân dân tỉnh Thái Nguyên*), Quy chế quản lý hoạt động và cung cấp thông tin của Cổng thông tin điện tử tỉnh Thái Nguyên *(theo Quyết định số 40/2012/QĐ-UBND ngày 06/11/2012 của Ủy ban nhân dân tỉnh Thái Nguyên),...*

b) Kiểm tra việc thực hiện các nội dung của Điều 4 về các biện pháp quản lý kỹ thuật cơ bản cho công tác an toàn, an ninh thông tin của cán bộ chuyên trách công nghệ thông tin;

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 bổ 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, Vi rút máy tính 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 về các biện pháp quản lý kỹ thuật cơ bản cho công tác an toàn, an ninh thông tin;

b) Tham mưu chuyên môn và vận hành an toàn hệ thống thông tin của đơn vị, triển khai các biện pháp đảm bảo 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 chuyên môn;

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 vi rút máy tính hoặc phần mềm gián điệp gây mất mát thông tin.

Điều 6. Xây dựng quy chế nội bộ đảm bảo an toàn cho hệ thống thông tin

1. Thủ trưởng các cơ quan, đơn vị được quy định tại Điều 2 của Quy chế này phải ban hành quy chế nội bộ, bảo đảm quy định rõ các vấn đề sau:

a) Mục tiêu và phương hướng thực hiện công tác đảm bảo an toàn an ninh cho hệ thống thông tin;

b) Nguyên tắc phân loại và quản lý mức độ ưu tiên đối với các tài nguyên của hệ thống thông tin (phần mềm, dữ liệu, trang thiết bị,…);

c) Quản lý phân quyền và trách nhiệm đối với từng cá nhân khi tham gia sử dụng hệ thống thông tin;

d) Quản lý và điều hành máy chủ, thiết bị mạng, thiết bị bảo vệ mạng một cách an toàn;

e) Kiểm tra, rà soát và khắc phục sự cố an toàn an ninh của hệ thống thông tin sử dụng các biện pháp trong Điều 4, Điều 5 và Điều 7 của Quy chế này;

f) Nguyên tắc chung sử dụng an toàn và hiệu quả đối với toàn bộ cá nhân tham gia sử dụng hệ thống thông tin;

g) Tổ chức thực hiện.

2. Các cơ quan, đơn vị xây dựng quy chế an toàn an ninh cho đơn vị căn cứ các tiêu chuẩn kỹ thuật quản lý an toàn của bộ tiêu chuẩn TCVN 7562:2005 và ISO/IEC 17799:2005 tại Phụ lục 1 để có sự lựa chọn áp dụng phù hợp với cơ quan mình.

Điều 7. Xây dựng và áp dụng quy trình đảm bảo an toàn, an ninh cho hệ thống thông tin

1. Các cơ quan nhà nước phải xây dựng và áp dụng quy trình đảm bảo an toàn, an ninh cho hệ thống thông tin nhằm giảm thiểu các nguy cơ gây ra sự cố, tạo điều kiện cho việc khắc phục và truy vết trong trường hợp có sự cố xảy ra.

Nội dung của quy trình nên chia làm các bước cơ bản sau:

a) Lập kế hoạch bảo vệ an toàn, an ninh cho hệ thống thông tin;

b) Xây dựng hệ thống bảo vệ an toàn, an ninh thông tin;

c) Quản lý và vận hành hệ thống bảo vệ an toàn, an ninh thông tin;

d) Kiểm tra đánh giá hoạt động của hệ thống bảo vệ an toàn, an ninh thông tin;

e) Bảo trì và nâng cấp hệ thống bảo vệ an toàn, an ninh thông tin.

2. Các cơ quan, đơn vị tham khảo các bước cơ bản để xây dựng khung quy trình đảm bảo an toàn, an ninh thông tin cho hệ thống thông tin tại Phụ lục 3 của Quy chế này và tiêu chuẩn quốc tế ISO 27001.

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

Điều 8. Trách nhiệm của các cơ quan, 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 thực hiện các quy định của pháp luật 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 cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông theo biểu mẫu tại Phụ lục 4 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 cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông để 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 5 của Quy chế này và gửi về Sở Thông tin và Truyền thông qua hộp thư điện tử vanthu.sotttt@thainguyen.gov.vn. Riêng báo cáo thuộc Quý IV của năm yêu cầu các đơn vị gửi về Sở Thông tin và Truyền thông bằng văn bản.

Điều 9. Trách nhiệm của cán bộ công chức, viên chức và người lao động trong các cơ quan, đơn vị

1. Nghiêm chỉnh chấp hành các quy định về bảo vệ bí mật nhà nước, quy chế nội bộ, quy trình về an toàn, an ninh thông tin của cơ quan, đơn vị cũng như quy định khác của pháp luật, nâng cao ý thức cảnh giác và trách nhiệm đảm bảo 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. Tham gia các chương trình đào tạo, hội nghị về an toàn, an ninh thông tin do Sở Thông tin và Truyền thông tổ chức.

Điều 10. Trách nhiệm của Công an tỉnh Thái Nguyên

1. Tham mưu cho Ủy ban nhân dân tỉnh chỉ đạo, tổ chức triển khai, thực hiện các Chỉ thị, Nghị quyết của Đảng, pháp luật Nhà nước về công tác bảo mệ bí mật nhà nước, bảo vệ an ninh chính trị nội bộ, an ninh kinh tế, an ninh thông tin, an toàn cơ sở hạ tầng, bảo vệ công trình quan trọng liên quan đến an ninh quốc gia, trật tự an toàn cơ quan; xây dựng, ban hành danh mục bảo vệ bí mật Nhà nước, các quy định về tiêu chuẩn, quy chuẩn kỹ thuật an toàn, an ninh thông tin trong vận hành, khai thác mạng lưới, dịch vụ, các công cụ phần cứng, chương trình virut, phần mềm gián điệp để phát tán thư rác, đánh cắp, sử dụng trái phép mật khẩu, khóa mật mã, lưu trữ, phát tán thông tin, tài liệu trái pháp luật, xâm phạm an toàn, an ninh thông tin, vi phạm thuần phong mỹ tục; thực hiện quyền, nghĩa vụ, trách nhiệm bảo vệ an ninh chính trị nội bộ, an ninh thông tin truyền thông, bảo vệ bí mật Nhà nước, an toàn cơ sở hạ tầng, trật tự an toàn cơ quan; làm tốt công tác chính trị tư tưởng, công tác quản lý nội bộ nhằm nâng cao ý thức trách nhiệm cho cán bộ công nhân viên; xây dựng phong trào " Toàn dân bảo vệ an ninh Tổ quốc".

2. Trao đổi kịp thời cho Sở Thông tin và Truyền thông và các cơ quan, đơn vị trên địa bàn tỉnh Thái Nguyên về âm mưu, phương thức, thủ đoạn hoạt động của các thế lực thù địch và tội phạm trên lĩnh vực viễn thông và công nghệ thông tin; nhằm phòng ngừa, ngăn chặn hoạt động của các thế lực thù địch và tội phạm; nâng cao tinh thần cảnh giác và ý thức trách nhiệm của cán bộ, công nhân viên.

3. Chỉ đạo các phòng nghiệp vụ và Công an các huyện, thành phố, thị xã tăng cường tuyên truyền vận động nhân dân các xã, phường, thị trấn có hệ thống thông tin đi qua nêu cao tinh thần trách nhiệm, ý thức cảnh giác, kịp thời ngăn chặn, phát hiện, tố giác những hành vi gây nguy hại đến công trình mạng lưới viễn thông, công nghệ thông tin. Triển khai công tác đảm bảo an ninh trật tự, phòng chống tội phạm và các hành vi vi phạm khác trong lĩnh vực viễn thông và công nghệ thông tin. Sau khi tiếp nhận tin báo về tội phạm xâm phạm an ninh trật tự trong lĩnh vực viễn thông và công nghệ thông tin phải khẩn trương tổ chức xác minh, điều tra làm rõ nguyên nhân, phương thức thủ đoạn, hoạt động của đối tượng, kịp thời đưa ra để xử lý theo pháp luật.

4. Khi phát hiện các thông tin, tài liệu, dữ liệu, đồ vật liên quan đến hoạt động xâm phạm an ninh quốc gia theo quy định tại Điều 3 Nghị định số 151/2005/NĐ-CP, ngày 14/12/2005 của Chính phủ quy định quyền hạn, trách nhiệm của cơ quan và cán bộ chuyên trách bảo vệ an ninh quốc gia, thực hiện ngay các biện pháp sau đây:

a) Yêu cầu tổ chức, cá nhân cung cấp các thông tin dữ liệu, số liệu, tài liệu, đồ vật liên quan;

b) Thực hiện theo thẩm quyền các biện pháp lưu giữ, sao chép thông tin, dữ liệu, tài liệu, đồ vật, một phần hoặc toàn bộ hệ thống thiết bị liên quan;

c) Ngăn cản việc truy nhập hệ thống thiết bị, mạng lưới và sử dụng dịch vụ;

d) Thực hiện các nhiệm vụ, quyền hạn khác theo quy định của pháp luật.

Điều 11. Trách nhiệm của Sở Thông tin và Truyền thông

1. Tham mưu UBND tỉnh về công tác đảm bảo an toàn, an ninh thông tin và chịu trách nhiệm trước UBND tỉnh trong việc đảm bảo an toàn, an ninh cho các hệ thống thông tin cấp tỉnh.

2. Xây dựng kế hoạch, dự toán nguồn kinh phí để triển khai công tác an toàn và an ninh thông tin phục vụ cho việc vận hành các hệ thống thông tin được UBND tỉnh giao quản lý và lưu ký các trang thông tin điện tử của các sở ngành, huyện, thành phố, thị xã.

3. Thành lập Đoàn kiểm tra an toàn, an ninh thông tin và tiến hành kiểm tra theo định kỳ hoặc đột xuất khi phát hiện có các dấu hiệu, hành vi vi phạm an toàn, an ninh thông tin. Kết thúc đợt kiểm tra phải có văn bản báo cáo UBND tỉnh về tình hình an toàn, an ninh thông tin thuộc tỉnh và có những đề xuất phù hợp.

4. Xây dựng và triển khai các chương trình đào tạo, hội nghị tuyên truyền an toàn, an ninh thông tin trong công tác quản lý nhà nước thuộc tỉnh nhằm phổ biến, cập nhật kiến thức về an toàn an ninh thông tin vào Quý III hằng năm.

5. Tùy theo mức độ sự cố, phối hợp Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố thông tin.

6. Hướng dẫn, giám sát các đơn vị xây dựng Quy chế đảm bảo an toàn, an ninh cho hệ thống thông tin theo quy định của nhà nước.

Chương IV
CÔNG TÁC THANH TRA, KIỂM TRA AN TOÀN, AN NINH THÔNG TIN

Điều 12. Kế hoạch kiểm tra hằng năm

1. Sở Thông tin và Truyền thông chủ trì, phối hợp Văn phòng UBND tỉnh, Công an tỉnh và các đơn vị có liên quan tiến hành công tác kiểm tra an toàn, an ninh thông tin tại tất cả các đơn vị hành chính cấp tỉnh, huyện, thành phố, thị xã định kỳ hằng năm tối thiểu 1 lần vào quý III, kiểm tra tại cơ sở cấp phường/xã theo kế hoạch của Sở Thông tin và Truyền thông.

2. Tiến hành kiểm tra đột xuất các cơ quan nhà nước khi có dấu hiệu vi phạm an toàn, an ninh thông tin.

Điều 13. Quan hệ phối hợp và trách nhiệm của các cơ quan chức năng liên quan

1. Sở Thông tin và Truyền thông

a) Chịu trách nhiệm chính trong việc chủ trì và phối hợp với các cơ quan chức năng liên quan để thành lập Đoàn kiểm tra và triển khai, báo cáo công tác kiểm tra an toàn, an ninh thông tin trên quy mô toàn tỉnh;

b) Phối hợp với Công an tỉnh thực hiện xử lý các hành vi vi phạm an toàn, an ninh thông tin gây thiệt hại cho hệ thống thông tin thuộc các cơ quan, đơn vị nhà nước thuộc tỉnh.

2. Văn phòng UBND tỉnh:

a) Cử bộ phận chuyên trách an toàn, an ninh thông tin phối hợp với Sở Thông tin và Truyền thông kiểm tra, đánh giá công tác an toàn, an ninh thông tin;

b) Phối hợp xây dựng các tiêu chí và quy trình kỹ thuật kiểm tra công tác an toàn, an ninh thông tin.

3. Trách nhiệm của Công an tỉnh:

a) Phối hợp Sở Thông tin và Truyền thông kiểm tra công tác an toàn, an ninh thông tin;

b) Tham mưu UBND tỉnh ban hành, sửa đổi, bổ sung các quy định của pháp luật có liên quan đến công tác an toàn, an ninh thông tin;

c) Thường xuyên thông báo cho các cơ quan, đơn vị về phương thức, thủ đoạn mới của các loại tội phạm xâm phạm an toàn, an ninh thông tin để có biện pháp phòng ngừa, đấu tranh, ngăn chặn;

d) Điều tra và xử lý các trường hợp vi phạm an toàn, an ninh thông tin theo thẩm quyền.

Chương V
KHEN THƯỞNG, XỬ LÝ VI PHẠM

Điều 14. Khen thưởng

Hằng năm, Sở Thông tin và Truyền thông dựa trên kết quả kiểm tra, đánh giá, 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 tỉnh xem xét khen thưởng cho các cá nhân, đơn vị có thành tích đảm bảo an toàn, an ninh thông tin theo quy định hiện hành.

Điều 15. Xử lý vi phạm

Tổ chức cá nhân có hành vi vi phạm quy chế này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật, xử phạt hành chính hoặc bị truy cứu trách nhiệm hình sự quy định của pháp luật hiện hành.

Chương VI

ĐIỀU KHOẢN THI HÀNH

Điều 16. Sở Thông tin và Truyền thông chủ trì, phối hợp với các sở, ban, ngành, UBND các huyện, thành phố, thị xã và các cơ quan có liên quan triển khai thực hiện Quy chế này.

Trong quá trình thực hiện, nếu có vướng mắc, đề nghị cơ quan, tổ chức, cá nhân có liên quan phản ánh về Sở Thông tin và Truyền thông tổng hợp trình UBND tỉnh xem xét, giải quyết./.

TM. ỦY BAN NHÂN DÂN TỈNH
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

(Đã ký)

Nhữ Văn Tâm

Phụ lục 1
10 NỘI DUNG CHÍNH CỦA ISO/IEC 17799:2005 DÙNG ĐỂ XÂY DỰNG QUY CHẾ NỘI BỘ ĐẢM BẢO AN TOÀN, AN NINH CHO HỆ THỐNG THÔNG TIN

(Ban hành kèm theo Quyết định số: 31/2013/QĐ/UBND ngày 16 tháng 12 năm 2013 của Uỷ ban nhân dân tỉnh Thái Nguyên)

1. Chính sách an toàn thông tin: Chỉ thị và hướng dẫn về an toàn thông tin.

2. An ninh tổ chức:

a) Hạ tầng an ninh thông tin: quản lý an ninh thông tin trong tổ chức;

b) An ninh đối với bên truy cập thứ ba: Duy trì an ninh cho các phương tiện xử lý thông tin của tổ chức và tài sản thông tin cho các bên thứ ba truy nhập.

3. Phân loại và kiểm soát tài sản:

a) Trách nhiệm giải trình tài sản: duy trì bảo vệ tài sản;

b) Phân loại thông tin tài sản: bảo đảm mỗi loại tài sản có mức bảo vệ thích hợp.

4. An ninh cá nhân:

a) An ninh trong định nghĩa công việc và nguồn nhân lực: giảm rủi ro do các hành vi sai sót của con người;

b) Đào tạo người sử dụng: bảo đảm người sử dụng nhận thức được các mối đe dọa và các vấn đề liên quan đến an ninh thông tin;

c) Đối phó các sự cố an ninh: Giảm thiểu thiệt hại từ các hỏng hóc, trục trặc và sự cố an ninh, theo dõi và rút kinh nghiệm.

5. An ninh môi trường vật lý:

a) Phạm vi an ninh: ngăn ngừa việc truy cập, gây hại và can thiệp trái phép vào vùng an ninh và thông tin nghiệp vụ;

b) An ninh thiết bị: để tránh mất mát, lỗi hoặc các sự cố khác liên quan đến tài sản gây ảnh hưởng đến các hoạt động nghiệp vụ;

c) Kiểm soát chung: ngăn ngừa làm hại hoặc đánh cắp thông tin và các phương tiện xử lý thông tin.

6. Quản lý truyền thông và hoạt động:

a) Thủ tục vận hành và trách nhiệm vận hành hệ thống: bảo đảm các phương tiện xử lý thông tin hoạt động đúng và an toàn;

b) Lập kế hoạch hệ thống và công nhận: giảm thiểu rủi ro về lỗi hệ thống;

c) Bảo vệ chống lại phần mềm cố ý gây hại: bảo vệ tính toàn vẹn của phần mềm hệ thống và thông tin;

d) Công việc quản lý: duy trì tính toàn vẹn và sẵn sàng của dịch vụ truyền đạt và xử lý thông tin;

e) Quản trị mạng: bảo đảm việc an toàn thông tin trên mạng và bảo vệ cơ sở hạ tầng kỹ thuật;

g) Trao đổi thông tin: Ngăn ngừa mất mát, thay đổi hoặc sử dụng sai thông tin được trao đổi giữa các đơn vị.

7. Kiểm soát truy cập:

a) Các yêu cầu nghiệp vụ đối với kiểm soát truy nhập: kiểm soát truy nhập thông tin;

b) Quản lý truy nhập của người dùng: Để tránh các truy nhập không được cấp phép vào hệ thống;

c) Trách nhiệm của người dùng: để tránh các truy nhập của người dùng không được cấp phép;

d) Kiểm soát truy nhập mạng: bảo vệ các dịch vụ mạng;

e) Kiểm soát truy nhập hệ điều hành: tránh truy nhập vào các máy tính không được phép;

g) Kiểm soát truy nhập ứng dụng: tránh các truy nhập trái phép vào hệ thống;

h) Giám sát truy nhập hệ thống và giám sát sử dụng hệ thống: để phát hiện các hoạt động không được cấp phép;

i) Kiểm soát truy nhập từ xa: bảo đảm an ninh thông tin khi sử dụng các phương tiện di động.

8. Phát triển và duy trì hệ thống:

a) Yêu cầu an ninh đối với các hệ thống: để bảo đảm các yêu cầu an ninh được đưa vào trong quá trình xây dựng hệ thống;

b) An ninh trong hệ thống ứng dụng: để ngăn ngừa mất mát, thay đổi hoặc lạm dụng dữ liệu người sử dụng trong các hệ thống ứng dụng;

c) Các kiểm soát mật mã, mã hóa: để bảo vệ tính tin cậy, xác thực hoặc toàn vẹn của thông tin;

d) An ninh các tệp hệ thống: Bảo đảm rằng các dự án CNTT và các hoạt động hỗ trợ được quản lý một cách an toàn;

e) An ninh quá trình hỗ trợ và phát triển: duy trì an ninh của phần mềm và thông tin hệ thống ứng dụng.

9. Quản lý liên tục trong kinh doanh: chống lại sự giám đoạn trong các hoạt động kinh doanh.

10. Sự tuân thủ:

a) Tuân thủ các yêu cầu pháp lý: để tránh các vi phạm của các Bộ luật hình sự và dân sự, các nghĩa vụ có tính luật pháp, nguyên tắc;

b) Chính sách an ninh và yêu cầu kỹ thuật của hệ thống phải bảo đảm việc tuân thủ các chính sách và tiêu chuẩn an ninh của quốc gia;

c) Xem xét kiểm tra hệ thống: để tối ưu tính hiệu lực nhằm giảm thiểu sự can thiệp quy trình kiểm tra hệ thống đó.

Phụ lục 2:
GIẢI THÍCH, GHI CHÚ TỪ TIẾNG ANH, TỪ KỸ THUẬT CHUYÊN NGÀNH

(Ban hành kèm theo Quyết định số: 31/2013/QĐ/UBND ngày 16 tháng 12 năm 2013 của Uỷ ban nhân dân tỉnh Thái Nguyên)

1. Clients/Server: Mô hình mạng máy con - máy chủ.

2. AP - AcessPoint: Điểm truy cập không dây được cấu hình đặc biệt các nút trên mạng cục bộ không dây (WLAN). Các điểm truy cập hoạt động như một máy phát trung tâm và nhận tín hiệu radio WLAN.

3. SSID - Service set identification: Tên định danh dịch vụ của mạng. Thông thường nếu trong mạng của bạn chỉ có nhiều Access Point (AP) thì khi bạn truy cập vào AP nào bạn sẽ chọn SSID tương ứng. Nói chung SSID là tên đặt cho mạng Wireless của mình để nhận dạng.

4. Logfile: Được hiểu là một tập tin để lưu trữ thông điệp được tạo ra bởi một ứng dụng, dịch vụ, hoặc hệ điều hành. Các thông điệp này được sử dụng để theo dõi các hoạt động được hoặc đã thực hiện. Các tệp tin nhật ký thường là các tập tin văn bản đơn giản (mã ASCII) và thường có một phần mở rộng là ".log".

5. VPN - Virtual Private Network: Mạng riêng ảo, là một mạng dành riêng để kết nối các máy tính của các công ty, tập đoàn hay các tổ chức với nhau thông qua mạng Internet công cộng.

6. Network File and Folder Sharing: Chức năng chia sẻ thông tin trên hệ điều hành.

7. Mã hóa ở mức hệ điều hành: Dùng các công cụ có sẵn của hệ điều hành cung cấp để tiến hành mã hóa và giải mã.

8. Backup (Sao lưu): Sao lưu dữ liệu được dùng để khôi phục lại dữ liệu tại thời điểm tiến hành sao lưu khi hệ điều hành bị hỏng.

9. Trojan (Vius Trojan) : một chương trình dạng vi rút, một kẻ làm nội gián trong máy tính của bạn đã giúp cho tên tin tặc (hacker) điều khiển máy tính của bạn, Trojan giúp tên tin tặc lấy những thông tin quý báu của bạn, thậm chí hắn có thể xóa hoặc định dạng lại cả ổ cứng của bạn nữa. Trojan có thể nhiễm vào máy của bạn qua tập tin gắn kèm thư điện tử mà bạn đã vô tình tải về và chạy thử, hoặc có lẫn trong những chương trình trò chơi, nhưng chương trình mà bạn không rõ nguồn gốc...

10. Worms (Sâu dữ liệu): giống như virus ngoài trừ việc nó có thể tự tái tạo. Nó không chỉ có thể nhân rộng mà không cần đến việc phải "đột kích" vào "bộ não" của file và nó cũng rất ưa thích sử dụng mạng để lây lan đến mọi ngóc ngách của hệ thống. Điều này có nghĩa là một computer worm có đủ khả năng để làm thiệt hại nghiêm trọng cho toàn thể mạng lưới, trong khi một virus chỉ thường nhắm đến các tập tin trên máy bị nhiễm.

11. Hosting (Dịch vụ cho thuê máy chủ): là một loại hình lưu trữ trên Internet cho phép các cá nhân, tổ chức truy cập được webiste của họ thông qua World Wide Web.

12. Firewall: Tường lửa - Là hệ thống rào chắn mà một số cá nhân, tổ chức, doanh nghiệp, cơ quan nhà nước lập ra nhằm ngăn chặn người dùng mạng Internet truy cập các thông tin không mong muốn hoặc/và ngăn chặn người dùng từ bên ngoài truy nhập các thông tin bảo mật nằm trong mạng nội bộ.

13. IDS/IPS: Thiết bị phát hiện/phòng chống xâm nhập.

14. WAF- Web Application Firewall: Mức ứng dụng web.

15. SQL Injection (lỗi nhúng mã): Xảy ra trong các ứng dụng như SQL, LDAP khi sử dụng dữ liệu không xác thực được gửi tới hệ thống biên dịch như một phần mã lệnh. Những dữ liệu này của kẻ tấn công có thể lừa hệ thống biên dịch thực hiện những mã lệnh độc hại hoặc giúp những kẻ tấn công thâm nhập đến dữ liệu quan trọng một cách trái phép.

16. Cross-Site Scripting (xss) (Thực thi mã Script xấu) : Xảy ra khi một ứng dụng tiếp nhận những dữ liệu không đáng tin cậy và gửi chúng đến cho trình duyệt web mà không qua xử lý và kiểm duyệt. XSS cho phép kẻ tấn công thực hiện những mã lệnh độc trên trình duyệt của người bị tấn công và lợi dụng ăn cắp phiên truy cập để mạo danh hoặc hủy hoại trang web hoặc lừa người sử dụng đi đến những trang web độc hại khác.

17. Broken Authentication and Session Management (Hư hỏng cơ chế chứng thực và quản lý phiên làm việc) : Những đoạn chương trình kiểm tra danh tính và quản lý phiên làm việc của người sử dụng thường được làm qua loa không đúng cách. Điều này giúp kẻ thâm nhập có thể ăn cắp mật mã, khóa, mã của các phiên làm việc (session tokens) hoặc tận dụng những lỗi khác để giả mạo danh tính người sử dụng.

18. Insecure Direct Object References (đối tượng tham chiếu thiếu an toàn): Xảy ra khi người phát triển để lộ một tham chiếu đến những đối tượng trong hệ thống như

các tập tin , thư mục, hay chìa khóa dữ liệu. Nếu chúng ta không có một hệ thống kiểm tra truy cập, kẻ tấn công có thể lợi dụng những tham chiếu này để truy cập dữ liệu một cách trái phép.

19. Cross Site Request Forgery (CSRF) (Giả mạo yêu cầu): Kiểu tấn công này ép buộc trình duyệt web của một người dùng đã đăng nhập gửi những yêu cầu giao thức web (HTTP) tới một trang web bị lỗi, bao gồm cookie của phiên truy cập và những thông tin tự động khác như thông tin đăng nhập. Cách thức này cho phép kẻ tấn công buộc trình duyệt web tạo ra những yêu cầu cho ứng dụng lỗi mà ứng dụng này không thể biết được đây là những yêu cầu giả mạo của kẻ tấn công.

20. Security Misconfiguration (Lỗi cấu hình bảo mật, sai sót cấu hình an ninh): Một cơ chế an ninh tốt cần phải hiệu chỉnh về an ninh và triển khai nó cho các ứng dụng , khuôn mẫu, máy chủ ứng dụng, máy chủ web,máy chủ dữ liệu và các ứng dụng nền tảng. Tất cả những thiết lập nên được đinh nghĩa, thực hiện bảo trì vì rất nhiều thứ không được triển khai với thiết lập an toàn mặc định. Các hiệu chỉnh cũng bao gồm cập nhật phần mềm và những thư viện được sử dụng bởi ứng dụng.

21. Failure to Restrict URL Access (Sai sót hạn chết truy cập) : Nhiều ứng dụng web kiểm tra quyền thực thi địa chỉ truy cập (URL) trước khi dựng các liên kết và nút nhấn được bảo vệ. Tuy nhiên ứng dụng cũng phải thực hiện kiểm tra tương tự mỗi khi những trang thông tin được truy cập trực tiếp, nếu không kẻ tấn công có thể giả mạo URL để truy cập vào những trang thông tin ẩn này.

Insecure Cryptographic Storage(Lưu trữ mật mã thiếu an toàn) : Nhiều ứng dụng web không bảo vệ những dữ kiệu nhạy cảm như thẻ tín dụng, số chứng minh nhân dân và những mã xác thực thông tin bằng phương thức mã hóa hay băm. Kẻ tấn công có thể ăn cắp hay thay đổi những dữ liệu nhạy cảm này và tiến hành hành vi trộm cắp, gian lận thẻ tín dụng, v.v…

22. Insufficient Transport Layer Protection (thiếu bảo vệ lớp vận chuyển): Các ứng dụng thường xuyên mắc sai lầm trong việc kiểm tra định danh, mã hóa và bảo vệ sự tuyệt mật và tính toàn vẹn của những thông tin nhạy cảm trên mạng lưới liên kết. Nó thường được bảo vệ bởi những thuật toán yếu, sử dụng những chứng nhận đã hết hiệu lực hoặc không sử dụng đúng cách.

23. Unvalidated Redirects and Forwards (Chuyển hướng và chuyển tiếp thiếu thẩm tra): Ứng dụng web thường xuyên đưa người dùng đến những liên kết qua các website khác và sử dụng những thông tin thiếu tin cậy để xác định đích đến. Nếu không được kiểm tra một cách cẩn thận, kẻ tấn công có thể lợi dụng để đưa nạn nhân

đến những trang web lừa đảo hay phần mềm độc hại, hoặc chuyển tiếp để truy cập các website trái phép.

24. Mirror : là một liên kết đến một bản sao của nội dung mà bạn đang nói về, chủ yếu là lưu trữ trên một máy chủ khác nhau để dự phòng.

RAID: là hình thức ghép nhiều ổ đĩa cứng vật lý thành một hệ thống ổ đĩa cứng có chức năng gia tăng tốc độ đọc/ghi dữ liệu hoặc nhằm tăng thêm sự an toàn của dữ liệu chứa trên hệ thống đĩa hoặc kết hợp cả hai yếu tố trên.

Clustering: Là một kiến trúc nhằm đảm bảo nâng cao khả năng sẵn sàng cho hệ thống mạng máy tính. Clustering cho phép sử dụng nhiều máy chủ kết hợp với nhau tạo thành một cụm có khả năng chịu đựng hay chấp nhận sai sót (fault - tolerant) nhằm nâng cao độ sẵn sàng của hệ thống mạng.

25. Trafic: Luồng dữ liệu.

26. Sharing: Chia sẻ tài nguyên.

27. Hacker: Được hiểu là người có thể viết hay chỉnh sửa phần mềm, phần cứng máy tính bao gồm lập trình, quản trị và bảo mật. Những người này hiểu rõ hoạt động của hệ thống máy tính, mạng máy tính và dùng kiến thức bản thân để làm thay đổi, chỉnh sửa nó với nhiều mục đích tốt xấu khác nhau.

28. Internet: Là hệ thống thông tin toàn cầu sử dụng giao thức Internet và tài nguyên Internet để cung cấp các dịch vụ và ứng dụng khác nhau cho người sử dụng dịch vụ viễn thông.

Phụ lục 3
CÁC BƯỚC CƠ BẢN ĐỂ XÂY DỰNG KHUNG QUY TRÌNH ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN CHO HỆ THỐNG THÔNG TIN

(Ban hành kèm theo Quyết định số: 31/2013/QĐ/UBND ngày 16 tháng 12 năm 2013 của Uỷ ban nhân dân tỉnh Thái Nguyên)

Bước 1: Lập kế hoạch bảo vệ an toàn an ninh cho hệ thống thông tin:

a) Thành lập bộ phận quản lý an toàn, an ninh thông tin;

b) Xây dựng định hướng cơ bản cho công tác đảm bảo an toàn, an ninh thông tin, trong đó chỉ rõ:

- Mục đích ngắn hạn và dài hạn;

- Phương hướng và văn bản pháp quy, tiêu chuẩn cần tuân thủ và tham khảo;

- Ước lượng nhân lực và kinh phí đầu tư.

c) Lập kế hoạch xây dựng hệ thống bảo vệ an toàn, an ninh thông tin:

- Xác định và phân loại các nguy cơ gây sự cố an toàn, an ninh thông tin;

- Rà soát và lập danh sách các đối tượng cần được bảo vệ với những mô tả đầy đủ về: nhiệm vụ; chức năng; mức độ quan trọng và các đặc điểm đối tượng (Đối tượng ở đây có thể là một phần mềm, các máy chủ, quy trình tác nghiệp thuộc cơ quan đơn vị…);

- Xây dựng phương án đảm bảo an toàn cho các đối tượng trong danh sách cần được bảo vệ: nguyên tắc quản lý, vận hành: các giải pháp bảo vệ và khắc phục sự cố…

- Liên lạc và hợp tác chặt chẽ Trung tâm Công nghệ thông tin và Truyền thông - Sở Thông tin và Truyền thông cũng như các cơ quan, tổ chức nghiên cứu và cung cấp dịch vụ toàn mạng;

- Lập kế hoạch dự trù kinh phí đầu tư cho hệ thống bảo vệ.

Bước 2: Xây dựng hệ thống bảo vệ an toàn an ninh thông tin:

- Tổ chức đội ngũ nhân viên chuyên trách, đủ năng lực đảm bảo an toàn, an ninh cho hệ thống thông tin;

- Xây dựng hệ thống bảo vệ an toàn an ninh thông tin theo kế hoạch.

Bước 3: Quản lý và vận hành hệ thống bảo vệ ATANTT:

- Vận hành và quản lý chặt chẽ trang thiết bị, phần mềm theo quy định đã đặt ra;

- Khi phát hiện sự cố cần nhanh chóng xác định nguyên nhân, tìm biện pháp khắc phục và báo cáo sự cố cho các cơ quan chức năng;

- Cài đặt đầy đủ, thường xuyên cập nhật phần mềm, các bản vá lỗi theo hướng dẫn của nhà cung cấp, thường xuyên thay đổi mật khẩu, sử dụng mật khẩu với độ an toàn cao.

Bước 4: Kiểm tra đánh giá hoạt động của hệ thống bảo vệ ATANTT:

- Thường xuyên kiểm tra giám sát các hoạt động của hệ thống bảo vệ an toàn, an ninh thông tin nói riêng cũng như toàn bộ hệ thống thông tin nói chung;

- Báo cáo tổng kết tình hình theo định kỳ.

Bước 5: Bảo trì và nâng cấp hệ thống bảo vệ ATANTT:

- Thường xuyên kiểm tra bảo trì hệ thống bảo vệ an toàn an ninh thông tin. Cần nhanh chóng mở rộng, nâng cấp hoặc thay thế khi cần thiết.

Phụ lục 4
MẪU BÁO CÁO SỰ CỐ

(Ban hành kèm theo Quyết định số: 31/2013/QĐ/UBND ngày 16 tháng 12 năm 2013 của Uỷ ban nhân dân tỉnh Thái Nguyên)

Đơn vị: ……..

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

Ngày …….tháng .....năm ……..

BÁO CÁO SỰ CỐ

1.Thông tin chung:

Đại diện lãnh đạo:.....

Tên cơ quan:.....

Email (cơ quan):.....

Điện thoại (cơ quan):.....

2.Thông tin về sự cố:

Số lượng máy chủ bị sự cố: .....Máy

Tên và chức năng chính của từng máy chủ:

Tên máy chủ 1: ……..

Hệ điều hành:

☐ Windows Phiên bản (Version):……..……..……..

☐ Linux Phiên bản (Version):…….……

☐ Ubutu Phiên bản (Version):…….……...……

☐ Khác: …….……..…

Chức năng:…….

Thời gian xảy ra sự cố: …/…../…./…./…./ (giờ/phút/ngày/tháng/năm)

Mô tả sơ bộ về sự cố: ……

…….

Các dịch vụ có trên Máy chủ (Đánh dấu những dịch vụ được sử dụng trên hệ thống)

☐ Web server ☐ Mail server ☐ Database server

☐ FPT server ☐ Proxy server ☐ Application server

☐ Dịch vụ khác, đó là:……

Địa chỉ IP của hệ thống:

☐ IP nội bộ với địa chỉ: …… - …… - ……- ……..……..

☐ IP ngoài với địa chỉ: …… - …… - ……- ……..……

Các tên miền của hệ thống:

……

Cách thức phát hiện: (Đánh dấu những hình thức phát hiện khi có sự cố)

☐ Người dùng cuối báo ☐ Quản trị hệ thống

☐ Qua hệ thống IDS/IPS ☐ Kiểm tra Log File

☐ Kiểm tra đường truyền ☐ Công ty, tổ chức tư vấn

☐ Khác, đó là……..

Các biện pháp đã xử lý khi gặp sự cố:

☐ Không làm gì cả ☐ Tự xử lý

☐ Báo cáo cấp trên ☐ Yêu cầu hỗ trợ từ nơi khác

☐ Hỗ trợ từ VNCERT ☐ Báo cáo cảnh sát mạng

☐ Khác, đó là……..

Đối với mỗi biện pháp, đề nghị mô tả cụ thể cách thức xử lý:

.....

.....

Tên máy chủ 2: ……..

Hệ điều hành:

☐ Windows Phiên bản (Version):……

☐ Linux Phiên bản (Version):……

☐ Ubutu Phiên bản (Version):……

☐ Khác: ……

Chức năng:…….

Thời gian xảy ra sự cố: …/…../…./…./…./ (giờ/phút/ngày/tháng/năm)

Mô tả sơ bộ về sự cố: ……

……

Các dịch vụ có trên Máy chủ (Đánh dấu những dịch vụ được sử dụng trên hệ thống)

☐ Web server ☐ Mail server ☐ Database server

☐ FPT server ☐ Proxy server ☐ Aplpication server

☐ Dịch vụ khác, đó là:……

Địa chỉ IP của hệ thống:

☐ IP nội bộ với địa chỉ: …… - …… - ……- ……..……..

☐ IP ngoài với địa chỉ: …… - …… - ……- ……..……

Các tên miền của hệ thống:

……..……

Cách thức phát hiện: (Đánh dấu những hình thức phát hiện khi có sự cố)

☐ Người dùng cuối báo ☐ Quản trị hệ thống

☐ Qua hệ thống IDS/IPS ☐ Kiểm tra Log File

☐ Kiểm tra đường truyền ☐ Công ty, tổ chức tư vấn

☐ Khác, đó là……..

Các biện pháp đã xử lý khi gặp sự cố:

☐ Không làm gì cả ☐ Tự xử lý

☐ Báo cáo cấp trên ☐ Yêu cầu hỗ trợ từ nơi khác

☐ Hỗ trợ từ VNCERT ☐ Báo cáo cảnh sát mạng

☐ Khác, đó là……..

.....

Tên máy chủ 3: ……..

Hệ điều hành:

☐ Windows Phiên bản (Version):……..……...……

☐ Linux Phiên bản (Version):…….……

☐ Ubutu Phiên bản (Version):…….....……

☐ Khác: …….……

Chức năng:…….

Thời gian xảy ra sự cố: …/…../…./…./…./ (giờ/phút/ngày/tháng/năm)

Mô tả sơ bộ về sự cố: ……

Các dịch vụ có trên Máy chủ (Đánh dấu những dịch vụ được sử dụng trên hệ thống)

☐ Web server ☐ Mail server ☐ Database server

☐ FPT server ☐ Proxy server ☐ Aplpication server

☐ Dịch vụ khác, đó là:……

Địa chỉ IP của hệ thống:

☐ IP nội bộ với địa chỉ: …… - …… - ……- ……..…..

☐ IP ngoài với địa chỉ: …… - …… - ……- ……..……

Các tên miền của hệ thống:.

…….……

Cách thức phát hiện: (Đánh dấu những hình thức phát hiện khi có sự cố)

☐ Người dùng cuối báo ☐ Quản trị hệ thống

☐ Qua hệ thống IDS/IPS ☐ Kiểm tra Log File

☐ Kiểm tra đường truyền ☐ Công ty, tổ chức tư vấn

☐ Khác, đó là……..

Các biện pháp đã xử lý khi gặp sự cố:

☐ Không làm gì cả ☐ Tự xử lý

☐ Báo cáo cấp trên ☐ Yêu cầu hỗ trợ từ nơi khác

☐ Hỗ trợ từ VNCERT ☐ Báo cáo cảnh sát mạng

☐ Khác, đó là……..

Phụ lục 5

MẪU BÁO CÁO TÌNH HÌNH AN TOÀN, AN NINH THÔNG TIN

(Ban hành kèm theo Quyết định số: 31/2013/QĐ/UBND ngày 16 tháng 12 năm 2013 của Uỷ ban nhân dân tỉnh Thái Nguyên)

Đơn vị: …….. **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
Độc lập - Tự do - Hạnh phúc

Ngày …….tháng .....năm …….

BÁO CÁO TÌNH HÌNH AN TOÀN, AN NINH THÔNG TIN

I. Đánh giá hiện trạng và dự kiến

1. Về chính sách, quản lý

Đơn vị:

+ Đã xây dựng kế hoạch để bảo đảm ATANTT cho tổ chức?

❍ Rồi (*đề nghị gửi kèm văn bản)* ❍ Chưa

+ Có các biện pháp vận hành liên tục và khôi phục sự cố không?

❍ Có ❍ Không

+ Có thường xuyên cập nhật công nghệ bảo đảm ATANTT hay không?

❍ Có ❍ Không

2. Về đầu tư

Đơn vị:

+ Phần trăm ngân sách trong tổng số ngân sách cho công nghệ thông tin để đầu tư vào việc đảm bảo an toàn thông tin …….%

+ Đã và dự kiến đầu tư vào lĩnh vực nào, năm nào dưới đây

Lĩnh vực	2013	Dự kiến năm 20.....	Mô tả nội dung
1. Xây dựng chính sách/ hướng dẫn/ thủ tục	☐	☐	
2. Sử dụng dịch vụ	☐	☐	

Lĩnh vực	2013	Dự kiến năm 20.....	Mô tả nội dung
3. Yêu cầu tư vấn	☐	☐	
4. Mua thiết bị an toàn thông tin	☐	☐	
5. Nghiên cứu sử dụng phần mềm mã nguồn mở	☐	☐	
6. Đào tạo nguồn nhân lực	☐	☐	
7. Các vấn đề khác:…….. ……..			

+ Đã và dự kiến sử dụng những công cụ nào, năm nào để bảo đảm ATANTT?

Công cụ	2012	Dự kiến 20…	Mô tả nội dung
1. Công cụ diệt Vi rút máy tính (Anti Vi rút máy tính)	☐	☐	
2. Mật khẩu	☐	☐	
3. Tường lửa	☐	☐	
4. Công cụ lọc thư rác	☐	☐	
5. Công cụ mã hóa tập tin	☐	☐	
6. Công cụ chống DDos			
7. Chữ ký điện tử	☐	☐	
8. Mạng riêng ảo (VPN)	☐	☐	
9. Hệ thống phát hiện xâm nhập	☐	☐	
10. Những công cụ khác:……..			

3. Về tình hình an ninh mạng và xử lý sự cố

+ Tổng kết về các sự cố an ninh mạng đã xảy ra trong năm 20… đối với đơn vị.

Sự cố	Đơn vị tính (Đợt, lần)	Số lượng
1. Vi rút máy tính		
2. Lừa đảo (Phishing)		
3. Thư rác (Spam mail)		
4. Spyware/ Adware		
5. Tấn công từ chối dịch vụ (Dos, Ddos)		
6. Nội dung Website đơn vị bị thay đổi (deface website)		
7. Sự cố khác: ……....		

+ Mức độ thiệt hại ước tính trong năm 20... do các sự cố ATANTT gây ra.

☐ Thiệt hại gián tiếp: …… triệu đồng

☐ Thiệt hại trực tiếp: …… triệu đồng

☐ Chi phí khắc phục: …… triệu đồng

+ Biện pháp xử lý đã áp dụng khi gặp sự cố.

Phương pháp	Số lần
1. Không làm gì cả	
2. Tự xử lý	
3. Báo cáo cấp trên trực tiếp	
4. Yêu cầu hỗ trợ từ nơi khác	
5. Báo cảnh sát mạng	
6. Phương pháp khác, đó là: ……... …….	

+ Cho biết công việc mà cơ quan đã thực hiện sau khi khắc phục được sự cố trong năm qua:

☐ Sửa đổi chính sách/ hướng dẫn/ thủ tục

☐ Nâng cao ý thức

☐ Tăng cường thiết bị

☐ Rà soát lại hệ thống

☐ Mở rộng lại liên kết với các đơn vị hoạt động trong lĩnh vực an toàn thông tin

☐ Việc khác đó là:

……

4. Tổ chức nhân lực và bồi dưỡng nghiệp vụ

+ Đơn vị có bộ phận phụ trách về bảo đảm ATANTT không?

○ Có ○ Không

+ Nếu có, bộ phận có người phụ trách là?

○ Lãnh đạo cơ quan ○ Giám đốc CNTT (CIO)

○ Cán bộ chuyên trách CNTT ○ Khác: ……

+ Nếu chưa có, thì đơn vị có dự kiến tổ chức bộ phận đó không?

○ Có ○ Không

Dự kiến sẽ triển khai thành lập vào tháng … năm ……, với số lượng cán bộ là … người.

+ Đơn vị có nhu cầu bồi dưỡng nghiệp vụ ATANTT?

☐ Dành cho lãnh đạo và cán bộ quản lý, số lượng dự kiến: … người

☐ Cơ bản/Nâng cao về ATANTT cho CB kỹ thuật, số lượng: … người

☐ Kỹ năng ATANTT cho người dùng , Số lượng dự kiến: …… người

+ Đơn vị đã có dự trù kinh phí cho huấn luyện nghiệp vụ, đào tạo phát triển nguồn nhân lực bảo đảm an ninh thông tin của đơn vị hay chưa?

○ Có ○ Chưa

+ Nếu tự đánh giá, mức độ ATANTT của đơn vị trong năm 20xx là:

Kém		Trung bình	Tốt		Rất tốt
❍ 0	❍ 1	❍ 2	❍ 3	❍ 4	❍ 5

II. Ý kiến phản hồi và góp ý thêm.

……

Chú ý:

- Điền thông tin đầy đủ vào các câu hỏi:

- Để lựa chọn đánh dấu X

- Câu hỏi với ký hiệu ❍ trước mối lựa chọn thì chỉ được phép đánh dấu một kết quả (chọn một)

- Câu hỏi với ký hiệu ☐ trước mỗi lựa chọn thì có thể đánh dấu từ không tới nhiều kết quả (chọn nhiều)

- Ký, ghi tên và đóng dấu đầy đủ vào cuối báo cáo và gửi về theo đường công văn cho Sở Thông tin và Truyền thông.