| | |
|---|---|
| UBND TỈNH BÌNH ĐỊNH<br>**SỞ CÔNG THƯƠNG** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**<br>**Độc lập – Tự do – Hạnh phúc** |
| Số: 140/QĐ-SCT | *Bình Định, ngày 22 tháng 10 năm 2014* |

# QUYẾT ĐỊNH
**V/v ban hành Quy chế đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin Sở Công Thương**

## GIÁM ĐỐC SỞ CÔNG THƯƠNG

Căn cứ Quyết định số 98/2009/QĐ-UBND ngày 21/01/2009 của UBND tỉnh về việc ban hành Quy định chức năng, nhiệm vụ quyền hạn và cơ cấu tổ chức của Sở Công Thương tỉnh Bình Định;

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 Chỉ thị số 897/CT-TTg ngày 10 tháng 6 năm 2011 của Thủ tướng Chính phủ về việc tăng cường triển khai các hoạt động đảm bảo an toàn thông tin số;

Căn cứ Quyết định số 22/2012/QĐ-UBND ngày 12 tháng 7 năm 2012 của UBND tỉnh Bình Định về việc Ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan quản lý hành chính nhà nước tỉnh Bình Định;

Xét đề nghị của Chánh Văn phòng Sở,

## QUYẾT ĐỊNH:

**Điều 1.** Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin Sở Công Thương.

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

**Điều 3.** Chánh Văn phòng Sở, Trưởng các Phòng chuyên môn, các đơn vị trực thuộc và cán bộ, công chức, viên chức của Sở Công Thương chịu trách nhiệm thi hành Quyết định này./-

***Nơi nhận:***
- Như điều 3;
- Lưu: VT, VP.

**GIÁM ĐỐC**

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ CÔNG THƯƠNG
TỈNH BÌNH ĐỊNH

**Nguyễn Kim Phương**

UBND TỈNH BÌNH ĐỊNH
**SỞ CÔNG THƯƠNG**

**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
**Độc lập – Tự do –Hạnh Phúc**

# QUY CHẾ
## Quy chế đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin Sở Công Thương

*(Ban hành kèm theo Quyết định số: 140 /QĐ-SCT ngày 22/ 10/2014 của Sở Công Thương)*

## Chương I
## NHỮNG QUY ĐỊNH CHUNG

### Điều 1. Phạm vi, đối tượng điều chỉnh

1. Quy chế này quy định về công tác đảm bảo an toàn, an ninh thông tin (viết tắt là ATANTT) trong hoạt động ứng dụng công nghệ thông tin (viết tắt là CNTT) của Sở Công Thương Bình Định.

2. Mọi cán bộ, công chức, viên chức (viết tắt là CBCCVC), các phòng, ban, đơn vị thuộc Sở; các cơ quan, tổ chức, cá nhân có quan hệ làm việc với Sở chịu sự điều chỉnh của Quy chế này.

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

1. Giảm thiểu được các nguy cơ gây sự cố mất an toàn thông tin và đảm bảo an ninh thông tin trong quá trình tác nghiệp của CBCCVC.

2. Công tác đảm bảo ATANTT, bảo mật trên môi trường mạng là một trong những nhiệm vụ trọng tâm để đảm bảo thành công trong việc ứng dụng CNTT trong hoạt động của các cơ quan quản lý hành chính nhà nước.

### Điều 3. Giải thích từ ngữ

Một số từ ngữ sử dụng trong Quy chế được hiểu như sau:

1. Quản trị mạng: 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 ATANTT 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: 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. Mạng LAN: là hệ thống mạng máy tính nội bộ của cơ quan.

7. FireWall: là một kỹ thuật được tích hợp vào hệ thống mạng để chống lại sự truy cập trái phép nhằm bảo vệ các nguồn thông tin nội bộ cũng như hạn chế sự xâm nhập vào hệ thông của một số hệ thống khác không mong muốn.

## Chương II
## QUY ĐỊNH BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN

### Điều 4. Về quản lý tài khoản người dùng

1. Quản trị mạng Sở có trách nhiệm tạo lập và cung cấp tài khoản truy nhập hệ thống mạng nội bộ, thư công vụ, văn phòng điện tử, dịch vụ công trực tuyến và một số hệ thống có liên quan khác cho CBCCVC của Sở.

Đối với công chức, viên chức tiếp nhận mới hoặc luân chuyển, ngừng công tác ở Sở: Quản trị mạng căn cứ Quyết định của cơ quan tạo mới hay hủy bỏ các tài khoản liên quan cho các cá nhân đó.

2. CBCCVC tự đặt lại mật khẩu tài khoản của mình (sau khi Quản trị mạng cung cấp tài khoản) đảm bảo tính bảo mật cao (Tối thiểu 8 ký tự, bao gồm chữ cái hoa, thường, chữ số và ký hiệu đặc biệt như: ! @ #,...), có trách nhiệm bảo vệ và bảo mật tài khoản, dữ liệu của mình; không tự ý xâm nhập các dữ liệu, tài khoản của người khác; đồng thời không cho thông tin tài khoản của mình cho các cá nhân khác không liên quan.

- Mật khẩu phải thay đổi định kỳ 3 tháng một lần hoặc đột xuất nếu cần thiết.

- Hạn chế tối đa việc sử dụng Internet công cộng để đăng nhập vào các tài khoản do Sở cấp.

### Điều 5. Về quản lý, sử dụng hệ thống

1. Đối với thiết bị CNTT:

- CBCCVC Sở có trách nhiệm quản lý trang thiết bị CNTT (máy vi tính, máy in, thiết bị ngoại vi, ...) được giao, tự quản lý dữ liệu trên máy tính của mình, tự quyết định việc chia sẻ tài nguyên với các máy tính khác theo đúng quy định. Ngoài ra, đối với cơ sở dữ liệu thuộc dạng tài liệu "Mật" theo quy định khi chia sẻ, cung cấp phải có ý kiến của lãnh đạo cơ quan và quản lý, lưu trữ theo quy định nhà nước.

- Quản trị mạng Văn phòng Sở và các đơn vị trực thuộc chịu trách nhiệm kiểm tra, theo dõi, đánh giá sự hoạt động của máy chủ, máy trạm, các thiết bị

mạng và các thiết bị ngoại vi theo đúng tiêu chuẩn kỹ thuật; thực hiện việc sao lưu dữ liệu chung; ghi nhật ký báo lỗi của mạng, các thiết bị CNTT để thực hiện công tác bảo trì, bảo dưỡng định kỳ, đột xuất, giảm thiểu tối đa các sự cố kỹ thuật.

- Máy tính chứa dữ liệu quan trọng và thường xuyên kết nối Internet phải cài đặt các phần mềm diệt virus tin cậy, có bản quyền.

- Máy tính và các thiết bị CNTT để nơi an toàn, tránh ảnh hưởng các tác nhân bên ngoài (ánh nắng, mưa...), không để các vật dụng, tài liệu dễ cháy nổ gần máy tính và các thiết bị ngoại vi nhằm tránh cháy nổ xảy ra, thường xuyên vệ sinh cho máy; hàng ngày sử dụng theo dõi sự hoạt động của máy tính, thiết bị ngoại vi... Khi không sử dụng máy tính nên tắt máy tính nhằm tiết kiệm điện và phòng, chống các xâm nhập trái phép.

- Trong quá trình sử dụng thiết bị CNTT, nếu có sự cố xảy ra, phòng chuyên môn lập tờ trình yêu cầu sửa chữa, chuyển đến Quản trị mạng.

2. Hệ thống mạng LAN:

- CBCCVC Sở khi tham gia vào mạng LAN không được tự ý thay đổi các tham số mạng, nếu tự ý thay đổi tham số mạng thì người thay đổi phải chịu hoàn toàn trách nhiệm. Trường hợp cần thiết phải thay đổi tham số mạng, báo cho Quản trị mạng biết để xử lý.

- Quản trị mạng chịu trách nhiệm cài đặt hệ thống an ninh mạng theo đúng tiêu chuẩn an toàn bảo mật; xử lý, khắc phục khi xảy ra sự cố máy tính bị Virus xâm nhập; đảm bảo hệ thống mạng máy tính luôn sạch virus để máy tính CBCCVC hoạt động tốt.

3. Quản lý Phòng máy chủ:

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

- Phòng máy chủ của Sở là khu vực hạn chế tiếp cận. Chỉ có Quản trị mạng hay những thành viên Lãnh đạo Sở cho phép mới được phép vào phòng máy chủ.

- 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 6. Phòng chống mã độc**

- 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.

- Các CBCCVC không được tự ý cài đặt hoặc gỡ bỏ các phần mềm trên máy trạm khi chưa có sự đồng ý của Quản trị mạng.

- 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.

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

- 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 Quản trị mạng để xử lý

**Điều 7. Cơ chế sao lưu dữ liệu**

1. Phân loại dữ liệu sao lưu:

- Dữ liệu hệ thống như: Website, Trang nội bộ, Văn phòng điện tử, Dịch vụ công trực tuyến, Thư công vụ, ...

- Các dữ liệu khác cài đặt trên máy tính cá nhân như: dữ liệu các phòng chuyên môn, số liệu quản lý thu chi kế toán, quản lý hồ sơ một cửa, cơ sở dữ liệu quản lý xuất nhập khẩu, cơ sở dữ liệu quản lý cụm công nghiệp, cơ sở dữ liệu quản lý cán bộ công chức, ...

2. Quy định thiết bị sao lưu:

- Đối với dữ liệu hệ thống: Sử dụng chức năng sao lưu dự phòng của các ứng dụng, kết hợp với sử dụng thiết bị lưu trữ tập trung ở Sở.

- Đối với các dữ liệu khác: Tùy vào mức độ quan trọng của dữ liệu CBCCVC sử dụng thiết bị nhớ gắn ngoài (ổ cứng di động, USB, đĩa CD, ...) nhằm lưu trữ dữ liệu an toàn và bảo mật.

3. Định kỳ sao lưu:

- Đối với dữ liệu hệ thống: 2 tuần/1 lần.

- Đối với các dữ liệu khác: sao lưu khi có sự thay đổi thông tin.

**Điều 8. Các hành vi bị nghiêm cấm**

1. Tạo ra, cài đặt, phát tán virus máy tính, phần mềm độc hại trái pháp luật.

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

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

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

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

6. Hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

**Điều 9. Giải quyết và khắc phục sự cố về ATANTT**

1. Đối với CBCCVC:

- Thông tin, báo cáo kịp thời cho Quản trị mạng và Văn phòng khi phát hiện các sự cố gây mất ATANTT trong hệ thống mạng.

- Xử lý khẩn cấp: Khi phát hiện hệ thống bị tấn công, thông qua các dấu hiệu khác thường như: hệ thống máy tính hoạt động chậm khác thường, nội dung bị thay đổi, … cần thực hiện những bước sau: Ngắt kết nối máy vi tính ra khỏi mạng LAN, Internet; Sao chép toàn bộ dữ liệu của hệ thống ra thiết bị lưu ngoài; Khôi phục hệ thống bằng dữ liệu đã sao lưu mới nhất để hệ thống hoạt động ổn định.

2. Đối với Quản trị mạng:

- Quản lý chặt chẽ việc di chuyển các trang thiết bị CNTT (máy chủ, máy trạm, thiết bị ngoại vi) của Sở.

- Hướng dẫn người dùng các biện pháp kỹ thuật giải quyết và khắc phục sự số; Trong trường hợp sự số xảy ra ngoài khả năng giải quyết, kịp thời báo cáo với lãnh đạo Sở; đồng thời phối hợp với cơ quan chuyên môn (Sở Thông tin và Truyền thông, Công an tỉnh,…) hướng dẫn khắc phục.

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

### Điều 10. Trách nhiệm của Lãnh đạo Sở

1. Lãnh đạo Sở có trách nhiệm trước UBND tỉnh trong công tác bảo vệ an toàn hệ thống thông tin của Sở.

2. Phân công cán bộ Quản trị mạng đảm bảo an toàn thông tin trước khi tiến hành các hoạt động quản lý, vận hành hệ thống thông tin.

3. Quan tâm đầu tư các thiết bị phần cứng, phần mềm liên qua đến công tác đảm bảo ATANTT. Bồi dưỡng, tuyển dụng nguồn nhân lực có kiến thức, trình độ về CNTT.

4. Khi có sự cố hoặc nguy cơ mất ATANTT, kịp thời cử cán bộ phối hợp chặt chẽ với cơ quan chuyên môn trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm ATANTT.

5. Chỉ đạo lãnh đạo các phòng tăng cường công tác ATANTT trong hoạt động ứng dụng CNTT và quan tâm đầu tư các thiết bị ATANTT ở đơn vị mình.

### Điều 11. Trách nhiệm của Văn phòng Sở

1. Hàng năm, lập Kế hoạch ứng dụng CNTT trong đó có Kế hoạch trang bị thiết bị, phần mềm ATANTT trình Lãnh đạo Sở phê duyệt thực hiện.

2. Kịp thời triển khai cho Sở những quy định, hướng dẫn có liên quan đến công tác ATANTT do cơ quan chuyên môn cấp trên ban hành.

### Điều 12. Trách nhiệm của Quản trị mạng tại Văn phòng Sở và đơn vị trực thuộc

1. Quản lý chặt chẽ việc di chuyển các thiết bị CNTT (Máy chủ, máy trạm, thiết bị ngoại vi), hệ thống mạng, thực hiện các báo cáo định kỳ về tình trạng hoạt động của toàn hệ thống mạng, đề nghị hướng giải quyết khi có sự cố. Thống kê, quản lý các thiết bị lưu trữ và sao lưu dữ liệu chung của đơn vị (như Website, trang nội bộ, Văn phòng điện tử, ...), đồng thời lập kế hoạch nâng cấp, thay thế các thiết bị khi không còn khả năng lưu trữ.

2. Thực hiện cấp phát, thu hồi, cập nhật và quản lý tất cả các tài khoản truy cập vào hệ thống thông tin của Sở; hướng dẫn người dùng thay đổi mật khẩu cá nhân theo quy định.

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

4. Quản lý, theo dõi các hoạt động thường xuyên và định kỳ như vận hành, sửa chữa hệ thống máy chủ, máy trạm, các thiết bị khác...; xử lý các yêu cầu về thay đổi tài khoản sử dụng mạng của các phòng chức năng, đơn vị thuộc Sở.

5. Sao lưu dữ liệu an toàn, kiểm tra dữ liệu sao lưu phải đảm bảo tính sẵn sàng và toàn vẹn.

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

**Điều 13. Đối với CBCCVC và người lao động**

1. Các máy tính khi không sử dụng trong thời gian dài (quá 2 giờ làm việc) cần tắt máy, để tránh bị 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.

2. Các CBCCVC có trách nhiệm tự quản lý các thiết bị CNTT được giao sử dụng; không tự ý thay đổi và tháo lắp các thiết bị trên máy vi tính khi chưa có sự đồng ý của Quản trị mạng; không tự ý liên hệ với cá nhân bên ngoài vào can thiệp các thiết bị máy tính.

3. Sử dụng chức năng mã hóa ở mức hệ điều hành bảo đảm các dữ liệu nhạy cảm như tài khoản, mật khẩu, các tệp văn bản, ... được mã hóa trước khi truyền trên môi trường mạng. Các tập tin gửi đính kèm bởi các 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.

4. Không được truy cập hoặc tải thông tin từ các Website độc hại, không được cài đặt các chương trình không rõ nguồn gốc, ...

5. Nghiêm chỉnh chấp hành các quy định nội bộ về ATANTT của cơ quan và các quy định khác của pháp luật; nâng cao ý thức cảnh giác và trách nhiệm, đảm bảo ATANTT tại cơ quan.

## Chương IV
## TỔ CHỨC THỰC HIỆN

**Điều 14. Khen thưởng và xử lý vi phạm**

1. Các phòng chuyên môn, đơn vị thuộc Sở; 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 trong việc đánh giá xếp loại cuối năm.

2. Các phòng chuyên môn, đơn vị thuộc Sở; 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.

**Điều 15. Trách nhiệm thi hành.**

Chánh Văn phòng, Chánh Thanh tra Sở, Trưởng các phòng chuyên môn, đơn vị thuộc Sở Công Thương có trách nhiệm tổ chức triển khai thực hiện Quy chế này. Trong quá trình thực hiện, nếu có những vấn đề vướng mắc, phát sinh bổ sung, sửa đổi đề nghị báo về Văn phòng Sở để giải quyết và trình Lãnh đạo Sở xem xét sửa đổi, bổ sung cho phù hợp.

**GIÁM ĐỐC**

CỘNG HOÀ X.H.C.N VIỆT NAM
SỞ CÔNG THƯƠNG
TỈNH BÌNH ĐỊNH

**Nguyễn Kim Phương**