UBND TỈNH BẮC GIANG **THANH TRA TỈNH**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 207 /QĐ-TTr	*Bắc Giang, ngày 16 tháng 10 năm 2023*

QUYẾT 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 Thanh tra tỉnh

CHÁNH THANH TRA TỈNH BẮC GIANG

Căn cứ Quyết định số 34/2020/QĐ-UBND ngày 14/10/2020 của UBND tỉnh Bắc Giang ban hành Quy chế bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước tỉnh Bắc Giang;

Căn cứ Quyết định số 747/2014/QĐ-UBND ngày 11/11/2014 của UBND tỉnh Bắc Giang ban hành Quy định chức năng, nhiệm vụ, quyền hạn của Thanh tra tỉnh Bắc Giang;

Theo đề nghị của Chánh văn phòng,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Thanh tra tỉnh.

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

Điều 3. Cán bộ, công chức, người lao động Thanh tra tỉnh và các tổ chức, cá nhân có liên quan căn cứ Quyết định thi hành./.

Nơi nhận:
- Như Điều 3;
- Sở Thông tin và Truyền thông;
- Lưu: VT.

CHÁNH THANH TRA

Trương Văn Nam

UBND TỈNH BẮC GIANG
THANH TRA TỈNH

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

QUY CHẾ
Đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Thanh tra tỉnh

(Ban hành kèm theo Quyết định số 207 /QĐ-TTr ngày 16 /10/2023 của Chánh Thanh tra tỉnh)

Chương I
QUY ĐỊNH CHUNG

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

1. Quy chế này quy định về công tác đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin (CNTT) của Thanh tra tỉnh bao gồm các hoạt động an toàn hạ tầng mạng, bảo đảm an toàn dữ liệu, an toàn thiết bị và các hệ thống thông tin, dữ liệu phục vụ các hoạt động của Thanh tra tỉnh.

2. Quy chế này được áp dụng với tất cả công chức, người lao động thuộc cơ quan và tổ chức, cá nhân có liên quan đến hoạt động ứng dụng CNTT của Thanh tra tỉnh

Điều 2. Mục đích, nguyên tắc đảm bảo an toàn thông tin

1. Việc áp dụng Quy chế này nhằm tăng cường năng lực phòng, chống các nguy cơ mất an toàn thông tin và đảm bảo an ninh thông tin trong quá trình ứng dụng CNTT trong hoạt động của cơ quan.

2. Các hoạt động ứng dụng CNTT phải tuân thủ theo Điều 3 Quy chế bảo đảm an toàn thông tin trong hoạt động ứng dụng CNTT của các cơ quan nhà nước tỉnh Bắc Giang được ban hành kèm theo Quyết định số 34/2020/QĐ-UBND ngày 14/10/2020 của UBND tỉnh Bắc Giang.

Chương II
QUY ĐỊNH ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 3. Quản lý và sử dụng trang thiết bị CNTT

1. Mỗi công chức, người lao động (người sử dụng) được trang bị các trang thiết bị CNTT phục vụ theo vị trí việc làm và định mức quy định của Nhà nước.

2. Người sử dụng có quyền và trách nhiệm trong việc khai thác, bảo quản, sử dụng hiệu quả trang thiết bị CNTT, không sử dụng vì mục đích riêng và không phục vụ theo yêu cầu công việc.

3. Mỗi trang thiết bị CNTT phải được dán nhãn ghi đầy đủ các thông tin cơ bản, ngày, tháng, năm sản xuất, bàn giao cho người sử dụng.

4. Người sử dụng trang thiết bị trước khi nghỉ chế độ, thay đổi đơn vị công tác, thôi việc... có trách nhiệm bàn giao lại nguyên trạng thiết bị, toàn bộ dữ liệu lưu trữ trên thiết bị (nếu có) cho Lãnh đạo phòng trước sự kiểm soát của coogn chức phụ trách CNTT.

5. Khi trang thiết bị CNTT phát sinh sự cố, việc xử lý sự cố tuân thủ Điều 7 tại Quy chế này.

Điều 4. Quản lý truy cập mạng LAN và WIFI

1. Tuyệt đối tuân thủ kiến trúc quy định của hệ thống, không tự ý lắp đặt, tháo dỡ các trang thiết bị, linh kiện mạng mà không có ý kiến của cán bộ được giao trách nhiệm quản lý bảo đảm an toàn thông tin.

2. Địa chỉ IP và địa chỉ Default Gateway là định danh duy nhất của máy tính cá nhân khi tham gia mạng nội bộ, mỗi cá nhân sử dụng máy tính trong mạng nội bộ không tự ý thay đổi các địa chỉ IP và địa chỉ Default gateway đã được cấp.

3. Mỗi tài khoản truy cập các hệ thống thông tin chỉ được cấp cho một người quản lý và sử dụng. Người sử dụng chịu trách nhiệm toàn diện đối với vấn đề bảo mật tài khoản cá nhân của mình. Trường hợp phát hiện ra truy nhập bất thường, hoặc bị chiếm đoạt tài khoản phải báo ngay cho bộ phận phụ trách.

4. Hạn chế việc sử dụng chức năng chia sẻ tài nguyên (sharing) trừ máy in, khi sử dụng chức năng này cần có chức năng bảo mật bằng mật khẩu và thực hiện việc thu hồi chức năng này khi đã sử dụng xong.

Điều 5. Sử dụng các Hệ thống thông tin và Thư điện tử công vụ

1. Không xâm nhập, sửa đổi, xóa bỏ nội dung thông tin của phòng, đơn vị và cá nhân khác.

2. Mỗi công chức, người lao động phải tự đặt mật khẩu đăng nhập vào các Hệ thống thông tin và Thư điện tử công vụ có độ phức tạp cao (độ dài tối thiểu 8 ký tự, bao gồm ký tự in thường, ký tự in hoa, ký tự số và ký tự đặc biệt như !, @, #, $, %,...) và định kỳ thay đổi nhằm tăng cường công tác bảo mật.

3. Không được truy cập vào các Trang thông tin điện tử không rõ về nội dung. Không đọc những thư điện tử không rõ nguồn gốc người gửi và kích hoạt các đường liên kết có dấu hiệu không rõ ràng.

4. Không tải những file đính kèm trên thư điện tử công vụ và các Trang thông tin khác không rõ nguồn gốc.

5. Nghiêm cấm việc lợi dụng Hệ thống thông tin để cung cấp, truyền đi, quảng bá hoặc đặt đường liên kết trực tiếp đến những thông tin chống lại Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam.

6. Nghiêm cấm đăng phát các hình ảnh phản cảm, thiếu tính nhân văn không phù hợp với thuần phong, mỹ tục Việt Nam.

7. Đối với các cá nhân nghỉ việc, chuyển công tác, bộ phận chuyên trách CNTT có trách nhiệm rà soát, thông báo và phối hợp các đơn vị liên quan để thu hồi tài khoản, xóa quyền truy cập vào các hệ thống thông tin.

Điều 6. Cài đặt các phần mềm ứng dụng

1. Tùy theo vị trí, công việc được giao, mỗi máy tính phục vụ công việc cho công chức và người lao động theo định mức hiện hành được phép cài đặt các phần mềm ứng dụng cần thiết phù hợp với nhu cầu công việc và yêu cầu đối với vị trí việc làm.

2. Trước khi máy tính được bàn giao phải được rà soát, quét mã độc.

3. Không tải và cài đặt các phần mềm không liên quan đến công việc chuyên môn lên máy tính cơ quan.

4. Việc cài đặt bổ sung các phần mềm cần phải được thực hiện sau khi có ý kiến của bộ phận chuyên trách CNTT.

5. Công chức, người lao động chịu toàn bộ trách nhiệm bảo đảm an toàn thông tin đối với chính máy tính do mình được giao quản lý, sử dụng.

Điều 7. Quản lý sự cố an toàn thông tin

1. Phân loại mức độ nghiêm trọng của sự cố

a) Thấp: Sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của các phòng thuộc cơ quan.

b) Trung bình: Sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của các phòng thuộc cơ quan.

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 các phòng thuộc cơ quan.

d) Khẩn cấp: Sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của các phòng thuộc cơ quan.

2. Xử lý sự cố

Khi có sự cố thì công chức, người lao động phải báo với bộ phận chuyên trách CNTT để kịp thời phối hợp xử lý.

Đối với sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của Thanh tra tỉnh thì công chức phụ trách CNTT báo cáo ngay Lãnh đạo cơ quan để phối hợp với Sở Thông tin và Truyền thông thực hiện theo quy trình từ Bước 4 (điểm c Khoản 4 Điều 11 Quy định ban hành kèm theo Quyết định số 34/2020/QĐ-UBND ngày 14/10/2020 của UBND tỉnh Bắc Giang).

Điều 8. Nhiệm vụ của công chức phụ trách CNTT

1. Tham mưu Lãnh đạo trì hoạt động ổn định của hệ thống mạng của cơ quan, đảm bảo hệ thống hoạt động an toàn, thông suốt, đáp ứng nhu cầu của người dùng và các quy định theo quy chế an toàn thông tin của tỉnh và các quy định có liên quan.

2. Là đầu mối tiếp nhận, hỗ trợ các sự cố có nguy cơ làm mất an toàn thông tin trong hoạt động của cơ quan.

3. Thường xuyên giám sát, nhắc nhở, khuyến cáo công chức, người lao động trong cơ quan tuân thủ các quy định tại Quy chế này và các quy định bảo đảm an toàn thông tin theo quy định hiện hành.

4. Thường xuyên cập nhật Quy định an toàn an ninh thông tin trong quá trình vận hành phòng hệ thống.

5. Tham mưu Lãnh đạo phối hợp với các cơ quan chuyên môn liên quan về công tác bảo đảm an toàn thông tin để triển khai các nhiệm vụ về an toàn thông tin theo quy định.

6. Là đầu mối triển khai các hoạt động nghiệp vụ nhằm bảo đảm an toàn thông tin trong nội bộ cơ quan.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 9. Trách nhiệm của công chức, người lao động trong cơ quan

1. Chịu trách nhiệm tuân thủ đầy đủ các nội dung được quy định tại Điều 12 Luật Công nghệ thông tin, Điều 7 Luật An toàn thông tin mạng, Điều 8 Luật An ninh mạng và các quy định của pháp luật có liên quan trong tất cả các hoạt động ứng dụng CNTT của cơ quan.

2. Nghiêm túc chấp hành quy chế này và các quy định khác của pháp luật về an toàn thông tin. Chịu trách nhiệm đảm bảo an toàn thông tin trong phạm vi trách nhiệm và quyền hạn được giao.

3. Mỗi công chức, người lao động phải có trách nhiệm tự quản lý, bảo quản thiết bị đã được giao sử dụng.

4. Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin phải báo cáo ngay với cấp trên và công chức phụ trách CNTT để kịp thời ngăn chặn và xử lý.

5. Tham gia các chương trình tập huấn về an toàn an ninh thông tin do cơ quan tổ chức.

6. Việc soạn thảo, đánh máy, in, sao chụp tài liệu mật phải thực hiện đúng Quy chế hiện hành của cơ quan và quy định của pháp luật về bảo vệ bí mật nhà nước có liên quan.

7. Các máy tính khi không sử dụng trong thời gian dài quá 02 giờ trở lên cần tắt máy, 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.

8. Tuyệt đối không cung cấp tài khoản, mật khẩu cho người khác ngoại trừ trường hợp cho phép theo quy định của pháp luật.

Điều 10. Trách nhiệm của các phòng nghiệp vụ, Văn phòng

1. Chánh văn phòng, Trưởng các phòng nghiệp vụ có trách nhiệm triển khai, tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trong công tác đảm bảo an toàn thông tin của phòng, đơn vị mình.

2. Thường xuyên tổ chức quán triệt các quy định về an toàn thông tin, nhằm nâng cao nhận thức về trách nhiệm đảm bảo an toàn thông tin.

3. Phân công một cán bộ thường xuyên theo dõi để đảm bảo an toàn thông tin của phòng.

4. Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố xảy ra một cách kịp thời, nhanh chóng và hiệu quả.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 11. Khen thưởng và xử lý vi phạm

1. Việc thực hiện tốt Quy chế này là một trong các tiêu chí để xem xét, đánh giá thi đua hằng năm của mỗi cá nhân.

2. Công chức, người lao động có hành vi vi phạm quy chế này và các quy định hiện hành của pháp luật thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật theo trách nhiệm hoặc bị truy cứu trách nhiệm hình sự. Nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật hiện hành.

3. Trong quá trình thực hiện nếu có phát sinh khó khăn, vướng mắc cần sửa đổi, bổ sung các phòng nghiệp vụ kịp thời phản ánh với công chức phụ trách CNTT để tổng hợp báo cáo Lãnh đạo cơ quan xem xét, điều chỉnh cho phù hợp./.