SỞ Y TẾ QUẢNG NINH
TRUNG TÂM KIỂM DỊCH Y TẾ QUỐC TẾ

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

Quảng Ninh, ngày 29 tháng 12 năm 2023

QUY CHẾ
Đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin

(Áp dụng từ 01/01/2024)

(Ban hành kèm theo Quyết định số: 203/QĐ-KDYT ngày 29 tháng 12 năm 2023 của Giám đốc Trung tâm Kiểm dịch Y tế quốc tế)

QUY ĐỊNH CHUNG

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

1. Quy chế này quy định các nội dung quản lý đảm bảo an toàn thông tin; các biện pháp quản lý kỹ thuật, vận hành đảm bảo an toàn thông tin đối với hệ thống thông tin trong các hoạt động ứng dụng công nghệ thông tin tại Trung tâm Kiểm dịch Y tế quốc tế Quảng Ninh.

2. Quy chế áp dụng đối với các cán bộ, viên chức và người lao động đang làm việc tại Trung tâm Kiểm dịch Y tế quốc tế Quảng Ninh trong việc vận hành, khai thác các ứng dụng công nghệ thông tin trong quản lý và điều hành.

Điều 2. Giải thích từ ngữ

1. Ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước: là việc sử dụng công nghệ thông tin vào các hoạt động quản lý nhằm nâng cao chất lượng, hiệu quả trong hoạt động công việc của cơ quan nhà nước và trong giao dịch của cơ quan nhà nước với tổ chức và cá nhân, hỗ trợ đẩy mạnh cải cách hành chính và bảo đảm công khai, minh bạch.

2. Hệ thống thông tin: là tập hợp các thiết bị viễn thông, công nghệ thông tin bao gồm phần cứng, phần mềm và cơ sở dữ liệu phục vụ cho hoạt động lưu trữ, xử lý, truyền đưa, chia sẻ, trao đổi, cung cấp và sử dụng thông tin.

3.Tài khoản người dùng (Account): bao gồm tên truy nhập (User name) và mật khẩu (Password) dùng để định danh và xác định quyền hạn sử dụng một dịch vụ nào đó khi đã đăng ký hoặc được cấp miễn phí với nơi cung cấp dịch vụ.

4. Trang thông tin điện tử (được gọi tắt là Website) là nơi cung cấp, trao đổi thông tin trên mạng Internet.

5. Thông tin cá nhân: Là thông tin đủ để xác định chính xác danh tính một cá nhân, bao gồm: Họ và tên, ngày sinh, nghề nghiệp, chức danh, địa chỉ liên hệ, địa chỉ thư điện tử, số điện thoại, số chứng minh nhân dân, số hộ chiếu. Những thông tin

thuộc bí mật cá nhân gồm có hồ sơ y tế, hồ sơ nộp thuế, số thẻ bảo hiểm xã hội, số tài khoản, số thẻ tín dụng và những bí mật cá nhân khác.

6. 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, bảo đảm kỹ thuật và an toàn, an ninh thông tin cho việc khai thác, vận hành hệ thống tại đơn vị.

7. Cán bộ thực hiện công tác đảm bảo an toàn thông tin: là cán bộ kỹ thuật hoặc quản lý kỹ thuật có chuyên môn về lĩnh vực CNTT trực tiếp làm công việc có liên quan đến đảm bảo an toàn thông tin tại đơn vị.

8. An toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin: là sự bảo vệ thông tin và các hệ thống thông tin luôn được bảo mật, sẵn sàng, toàn vẹn dữ liệu và không bị sử dụng, truy cập trái phép, gián đoạn.

9. Vi-rút máy tính là những chương trình hay đoạn mã mà được thiết kế để tự nhân bản và sao chép chính nó vào các đối tượng lây nhiễm khác (file, ổ đĩa, máy tính…).

10. Môi trường mạng bao gồm: mạng không dây(Wireless); mạng nội bộ (LAN); mạng diện rộng (WAN); mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước (TSLD); mạng riêng ảo (VPN); mạng Intranet; mạng Internet.

11. Nguy cơ mất an toàn thông tin: là những nhân tố bên ngoài hoặc bên trong có khả năng ảnh hưởng tới trạng thái an toàn thông tin.

12. Đánh giá rủi ro an toàn thông tin là việc xác định, phân tích nguy cơ mất an toàn thông tin có thể có và dự báo mức độ, phạm vi ảnh hưởng và khả năng gây thiệt hại khi xảy ra sự cố mất an toàn thông tin.

Điều 3. Tiêu chuẩn sử dụng.

1. Các thông tin, dữ liệu dạng ký tự quy định sử dụng để nhập số liệu trong hoạt động ứng dụng công nghệ thông tin tại cơ quan nhà nước là bộ mã ký tự chữ Việt theo Tiêu chuẩn Việt Nam TCVN 6909:2001 và phải được nhập bằng cách dùng bộ gõ chữ Việt Unicode.

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

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

4. 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
QUY ĐỊNH ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 4: Quản lý kỹ thuật, vận hành cơ bản của hệ thống thông tin tại Trung tâm Kiểm dịch Y tế quốc tế Quảng Ninh:

1. Trang bị đầy đủ các kiến thức bảo mật cơ bản cho cán bộ, viên chức và người lao động trước khi cho phép truy nhập và sử dụng hệ thống thông tin.

2. Hệ thống thông tin của cơ quan phải được triển khai cơ chế bảo mật và an toàn thông tin bằng các thiết bị phần cứng và phần mềm:

- Đầu tư trang bị các thiết bị phần cứng về bảo mật (firewall) phù hợp với quy mô hệ thống của cơ quan.

- Sử dụng phần mềm chống vi-rút máy tính có bản quyền và tin cậy trên các thiết bị mạng và máy tính quan trọng chứa dữ liệu.

3.Hệ thống thông tin luôn luôn có cơ chế sao lưu hoạt động thường xuyên, ổn định, đảm bảo các yêu cầu kỹ thuật quy định và an toàn ở các mức độ; hạn chế việc sử dụng chức năng chia sẻ tài nguyên, khi sử dụng chức năng này cần bật thuộc tính bảo mật bằng mật khẩu và thu hồi chức năng này khi đã sử dụng xong.

4. Hệ thống thông tin phải được triển khai chức năng giám sát truy cập từ ngoài vào hệ thống, từ hệ thống gửi ra bên ngoài, có khả năng ghi lại nhật ký hoạt động hệ thống để phục vụ công tác điều tra, quản lý, khắc phục sự cố và làm rõ nguyên nhân gây mất an toàn thông tin; chức năng ngăn chặn truy cập một số Website không phù hợp với Quy định hiện hành của Nhà nước.

5. Các hệ thống thông tin cần đặt các lớp bảo vệ bằng mật khẩu ở mức độ cao, có cơ chế xác minh người dùng; cần giới hạn một số hữu hạn lần đăng nhập sai liên tiếp.

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. Xác định cấu trúc thiết kế website; 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).

8. Phải đặt mật khẩu cho máy tính (mật khẩu đăng nhập, mật khẩu bảo vệ màn hình). Sử dụng các thiết bị lưu trữ thông tin (USB, ổ cứng gắn ngoài, thẻ nhớ...) đảm bảo an toàn, đúng cách để phòng ngừa virus, phần mềm gián điệp xâm nhập máy tính phá hoại, đánh cắp thông tin.

9. Thường xuyên cập nhật cấu hình chuẩn cho các thành phần của hệ thống thông tin, thiết lập cấu hình chặt chẽ nhất nhưng vẫn đảm bảo duy trì hoạt động thường xuyên của hệ thống thông tin.

10. Khi thiết lập cấu hình hệ thống thông tin chỉ cung cấp những chức năng thiết yếu nhất; xác định các chức năng, cổng giao tiếp mạng, giao thức, và dịch vụ không cần thiết để cấm hoặc hạn chế sử dụng.

Điều 5: Quy định quản lý kỹ thuật về công tác bảo vệ bí mật nhà nước về an toàn thông tin trên môi trường mạng:

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. Hệ thống mạng không dây (wireless) của cơ quan phải được thiết lập khóa khi truy cập, được phân định riêng mạng không dây nội bộ với mạng không dây dành cho khách truy cập.

3. Mạng riêng ảo (VPN) của cơ quan kết nối để truy cập vào hệ thống thông tin, kho lưu trữ dữ liệu phải được bảo mật, quản lý, kiểm soát chặt chẽ các kết nối, kiểm tra xác thực tài khoản truy cập và hủy bỏ kết nối khi không còn sử dụng.

4. Nghiêm cấm truy cập trái phép vào các máy tính, mạng máy tính, cơ sở dữ liệu không thuộc thẩm quyền, phân cấp của mình; không thực hiện các biện pháp nhằm vô hiệu hóa hệ thống giám sát, bảo mật thông tin, dữ liệu tại các thiết bị, máy tính của cơ quan.

5. Các máy tính khi không sử dụng trong thời gian dài (quá 4 giờ làm việc) cần tắt máy hoặc ngưng kết nối mạng, để tránh bị các tin tặc lợi dụng, sử dụng chức năng điều khiển từ xa dùng máy tính của mình tấn công vào các hệ thống thông tin khác.

6. Không truy cập vào các trang thông tin hay địa chỉ lạ trên mạng internet có tiềm ẩn các mã độc, mã phá hoại; phải thực hiện quét virus trước khi mở các tập tin đính kèm theo thư điện tử, không mở các thư điện tử khi chưa rõ người gửi hoặc tập tin đính kèm có nguồn gốc không rõ ràng để tránh virus, phần mềm gián điệp lây nhiễm máy tính.

7. Hệ thống thông tin tại cơ quan cần có cơ chế ngăn chặn hoặc hạn chế các sự cố gây ra do tấn công từ chối dịch vụ (DoS, DDoS). Sử dụng các thiết bị để lọc các gói tin nhằm bảo vệ các thiết bị bên trong, tránh bị ảnh hưởng trực tiếp bởi tấn công từ chối dịch vụ. Đối với hệ thống thông tin cho phép truy nhập công cộng có thể thực hiện bảo vệ bằng cách tăng dung lượng, băng thông hoặc thiết lập hệ thống dự phòng.

Điều 6: Cơ chế sao lưu dữ liệu:

1. Cơ chế sao lưu dữ liệu của hệ thống thông tin được đặt ở mức độ hệ thống, dữ liệu của ứng dụng, dữ liệu của người sử dụng; cơ chế sao lưu dữ liệu phải được thực hiện thường xuyên; thiết bị lưu trữ dữ liệu được sao lưu đảm bảo yêu cầu kỹ thuật; dữ liệu được sao lưu phải đảm bảo tính sẵn sàng và toàn vẹn đáp ứng yêu cầu phục hồi dữ liệu cho hệ thống thôn tin hoạt động bình thường khi có sự cố xảy ra. Quản lý chặt chẽ việc di chuyển các trang thiết bị công nghệ thông tin lưu trữ các thông tin thuộc danh mục bí mật nhà nước.

2. Người dùng phải quản lý và bảo mật các thông tin được lưu trên máy tính thông qua việc cài đặt các quyền truy cập vào từng danh mục dữ liệu trên máy tính.

3. Sử dụng các biện pháp bảo mật để ngăn chặn sự truy cập bất hợp pháp từ người dùng ngoài cũng như bên trong cơ quan vào hệ thống lưu trữ, sao lưu dữ liệu của hệ thống.

4. Các thiết bị lưu trữ cần được bảo quản ở nơi an ninh tốt, đảm bảo yêu cầu phòng chống cháy, nổ, áp suất, nhiệt độ, độ ẩm, ngoại lực, bụi, hóa chất...

5. Không lưu trữ các tài liệu có nội dung bí mật trên thiết bị di động thông minh. Không mang các thiết bị di động, thiết bị có chức năng ghi, sao chép, chụp ảnh, có kết nối internet vào các cuộc họp có nội dung bí mật. Không đăng nhập, sử dụng tài khoản hòm thư công vụ, đặng nhập vào các dịch vụ trực tuyến, truy cập VPN, đăng nhập vào các phần mềm quản lý thông tin cơ quan, nhà nước từ các máy tính, thiết bị lạ, kém bảo mật, không có độ tin cậy cao.

Điều 7: Giải quyết và khắc phục sự cố về an toàn thông tin:

1. Đối với người sử dụng:

a. Thông tin, báo cáo kịp thời cho cán bộ chuyên trách về công nghệ thông tin hoặc cán bộ thực hiện công tác đảm bảo an toàn thông tin của của Trung tâm Kiểm dịch Y tế quốc tế Quảng Ninh khi phát hiện các sự cố gây mất an toàn thông tin trong quá trình tham gia vào hệ thống thông tin của đơn vị.

b. Phối hợp tích cực trong quá trình giải quyết và khắc phục sự cố.

2. Đối với cán bộ chuyên trách về công nghệ thông tin, cán bộ thực hiện công tác đảm bảo công nghệ thông tin:

a. Khẩn trương triển khai các biện pháp kỹ thuật để giải quyết và khắc phục sự cố; đồng thời báo cáo sự cố và kết quả khắc phục sự cố cho Lãnh đạo đơn vị và lãnh đạo phòng.

b.Trong trường hợp sự cố xảy ra ngoài khả năng giải quyết của cơ quan hoặc cần sự trợ giúp trực tiếp cần:

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

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).

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

CHƯƠNG III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 8: Trách nhiệm của Lãnh đạo đơn vị, lãnh đạo cấp Khoa/phòng:

1. Lãnh đạo đơn vị :

a. Quán triệt và chỉ đạo thống nhất đối với cán bộ, viên chức và NLĐ trong đơn vị về đảm bảo an toàn, an ninh thông tin và công tác bảo vệ bí mật nhà nước, bảo vệ bí mật nội bộ trong quá trình vận hành, khai thác và sử dụng hệ thống thông tin tại cơ quan.

b. Tổ chức xây dựng và ban hành "Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Trung tâm Kiểm dịch Y tế quốc tế Quảng Ninh"; phân công cán bộ làm công tác công nghệ thông tin theo dõi, hướng dẫn việc đảm bảo an toàn thông tin tại cơ quan.

c. Quan tâm đầu tư các thiết bị phần cứng, phần mềm liên quan đến công tác đảm bảo an toàn thông tin.

2. Lãnh đạo cấp khoa, phòng:

a. Lãnh đạo các khoa, phòng phải thường xuyên tham gia và nhắc nhở các cán bộ, viên chức và người lao động của phòng thực hiện đúng qui chế và các qui định khác có liên quan.

b. Tạo điều kiện cho cán bộ, viên chức và người lao động và cán bộ chuyên trách công nghệ thông tin tham gia các buổi tập huấn quản lý, bảo mật, bồi dưỡng chuyên môn trong lĩnh vực an toàn thông tin.

c. Khi có sự cố hoặc nguy cơ mất an toàn thông tin phải chỉ đạo khắc phục sự cố kịp thời và hạn chế thấp nhất mức thiệt hại có thể xảy ra, đồng thời lập biên bản và báo cáo bằng văn bản về Văn phòng Trung tâm để giải quyết.

Điều 9: Trách nhiệm cán bộ chuyên trách công nghệ thông tin và cán bộ thực hiện công tác đảm bảo an toàn thông tin:

1. Cán bộ phụ trách công nghệ thông tin phải hướng dẫn, hỗ trợ kỹ thuật cơ bản cho cán bộ, viên chức và người lao động tại cơ quan nhằm thực hiện đảm bảo an toàn thông tin trong hệ thống thông tin.

2. Thường xuyên rà soát, cập nhật cập nhập các lỗi bảo mật, cấu hình hệ thống với với những chính sách bảo mật phù hợp hoạt động hệ thống thông tin đơn vị, các giải pháp, sáng kiến tăng cường công tác bảo mật thông tin.

3. Thực hiện thu hồi và vô hiệu hóa sử dụng tất cả các tài khoản, thiết bị dụng để truy cập hệ thống, chứa dữ liệu, tài liệu của cán bộ, viên chức và người lao động ngay sau khi ngừng công tác tại đơn vị;

4. Thường xuyên sao lưu dữ liệu quan trọng, các cơ sở dữ liệu theo đúng quy định và định kỳ hàng tháng; kiểm tra dữ liệu sao lưu phải đảm bảo tính sẵn sàng, toàn vẹn của dữ liệu.

5. Hỗ trợ, thông báo cho lãnh đạo đơn vị và Lãnh đạo Khoa/phòng về sự cố hoặc nguy cơ xảy ra sự cố có ảnh hưởng đến việc quản lý và sử dụng hệ thống.

6. Tổ chức kiểm tra thường quy và đột xuất tại các phòng để đánh giá và có cơ sở kiến nghị Thủ trưởng cơ quan khen thưởng hoặc phê bình phòng hoặc cá nhân trong việc thực hiện Quy chế an toàn thông tin.

Điều 10: Trách nhiệm của cán bộ công chức, viên chức và người lao động:

1. Học tập, nghiên cứu các tài liệu ban hành quy định về bảo đảm an toàn hệ thống thông tin; tham gia và tìm hiểu các buổi tuyên truyền nâng cao ý thức về bảo vệ bí mật nhà nước, bảo vệ thông tin trong hoạt động ứng dụng công nghệ thông tin.

2. Báo cáo kịp thời và chủ động phối hợp với cán bộ chuyên trách công nghệ thông tin kiểm tra và khắc phục sự cố về an toàn thông tin trong quá trình làm việc.

3. Tuân thủ theo hướng dẫn kỹ thuật đã ban hành của Trung tâm Kiểm dịch Y tế quốc tế Quảng Ninh và các quy định khác của nhà nước về đảm bảo an toàn thông tin. Nâng cao ý thức cảnh giác và trách nhiệm về an toàn thông tin.

4. Chỉ được sử dụng tài khoản của mình được cung cấp để đăng nhập vào hệ thống thông tin; tự bảo vệ mật khẩu đăng nhập và không để người khác sử dụng tài khoản của mình để đăng nhập hệ thống.

5. Không truy cập và sử dụng thông tin cơ quan cho cho việc đăng ký thông tin trên mạng với mục đích thương mại, mục đích cá nhân.

6. 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.

7. 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 V
ĐIỀU KHOẢN THI HÀNH

Điều 11. Công tác kiểm tra

Giám đốc Trung tâm Kiểm dịch Y tế quốc tế Quảng Ninh tổ chức kiểm tra định kỳ năm hoặc đột xuất việc thực hiện Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin tại cơ quan theo đúng quy định.

Điều 12: Điều khoản thi hành

1. Cán bộ, viên chức và người lao động quy định tại khoản 2, Điều 1 của Quy chế này chịu trách nhiệm tổ chức thực hiện.

2. Phòng KHTH, cán bộ Công nghệ thông tin hướng dẫn, kiểm tra việc thực hiện Quy chế này.

3. Trong quá trình thực hiện Quy chế, nếu có vướng mắc cần sửa đổi, bổ sung, các phòng chức năng phản ánh về Phòng KHTH, Cán bộ công nghệ thông tin để tổng hợp, trình Giám đốc xem xét, quyết định./.

GIÁM ĐỐC

SỞ Y TẾ TỈNH QUẢNG NINH
TRUNG TÂM KIỂM DỊCH Y TẾ QUỐC TẾ

Hoàng Văn Lương