BỘ XÂY DỰNG
CỤC HÀNG KHÔNG VIỆT NAM

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

Số: 1986 /QĐ-CHK

Hà Nội, ngày 23 tháng 10 năm 2025

QUYẾT ĐỊNH
Ban hành Quy chế sử dụng mạng máy tính nội bộ, mạng máy tính có kết nối Internet của Cục Hàng không Việt Nam

CỤC TRƯỞNG CỤC HÀNG KHÔNG VIỆT NAM

Căn cứ Luật Cơ yếu số 05/2011/QH13 ngày 26 /11/2011;

Căn cứ Luật Bảo vệ bí mật nhà nước ngày 15/11/2018;

Căn cứ Nghị định số 26/2020/NĐ-CP ngày 28/02/2020 của Chính phủ quy định chi tiết một số điều của Luật Bảo vệ bí mật nhà nước;

Căn cứ Quyết định số 09/QĐ-BXD ngày 01/03/2025 của Bộ trưởng Bộ Xây dựng quy định chức năng nhiệm vụ, quyền hạn và cơ cấu tổ chức của Cục Hàng không Việt Nam;

Căn cứ Quyết định số 43/QĐ-CHK ngày 10/03/2025 của Cục trưởng Cục Hàng không Việt Nam quy định chức năng nhiệm vụ, quyền hạn của các Phòng, Thanh tra, Văn phòng thuộc Cục Hàng không Việt Nam;

Căn cứ Quyết định số 745/QĐ-BXD ngày 03/6/2025 của Bộ trưởng Bộ Xây dựng Ban hành Quy chế quản lý, vận hành, khai thác và bảo đảm an toàn thông tin mạng Hệ thống quản lý văn bản, Trục liên thông văn bản Bộ Xây dựng;

Căn cứ Kết luận số 29/KL-X05 ngày 17/12/2024 của Thanh tra Bộ Công an về thanh tra việc chấp hành các quy định của pháp luật về bảo vệ bí mật nhà nước và an ninh mạng đối với Bộ Giao thông vận tải;

Theo đề nghị của Trưởng phòng Phòng Khoa học, Công nghệ và Môi trường.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế sử dụng mạng máy tính nội bộ, mạng máy tính có kết nối Internet của Cục Hàng không Việt Nam.

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

Điều 3. Chánh Văn phòng, Chánh Thanh tra, các Trưởng phòng thuộc Cục Hàng không Việt Nam và thủ trưởng các cơ quan, đơn vị, cá nhân liên quan liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ Xây dựng (để b/c);
- Trung tâm CNTT – Bộ Xây dựng;
- Cục X05, A03, A04, A05 - Bộ Công an;
- Các Phó Cục trưởng (để chỉ đạo);
- Lưu: VT, KHCNMT

CỤC TRƯỞNG

BỘ XÂY DỰNG
CỤC HÀNG KHÔNG VIỆT NAM

Lương Việt Dũng

QUY CHẾ

Sử dụng mạng máy tính nội bộ, mạng máy tính có kết nối Internet của Cục Hàng không Việt Nam

(Kèm theo Quyết định số 1982/QĐ-CHK ngày 23 tháng 10 năm 2025 của Cục trưởng Cục Hàng không Việt Nam)

CHƯƠNG I: QUY ĐỊNH CHUNG

Điều 1. Phạm vi và đối tượng áp dụng

1. Phạm vi

Quy chế này quy định về bảo đảm an toàn thông tin và an ninh mạng trong Sử dụng mạng máy tính nội bộ, mạng máy tính có kết nối Internet của Cục Hàng không Việt Nam.

2. Đối tượng áp dụng

Quy chế này áp dụng đối với các phòng thuộc Cục Hàng không Việt Nam và đơn vị trực thuộc Cục Hàng không Việt Nam (sau đây gọi chung là "đơn vị").

Cán bộ, công chức, viên chức và người lao động làm việc trong các cơ quan, đơn vị trực thuộc Cục Hàng không Việt Nam (sau đây gọi chung là "cá nhân").

Các tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin, an toàn thông tin, an ninh mạng hoặc tham gia kết nối với hệ thống thông tin của Cục Hàng không Việt Nam.

Điều 2. Giải thích từ ngữ

Trong Quy chế này, các thuật ngữ được hiểu như sau:

An toàn thông tin: Là việc bảo vệ thông tin và các hệ thống thông tin tránh bị truy cập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép, sử dụng sai mục đích nhằm đảm bảo tính bảo mật, toàn vẹn và khả dụng của thông tin.

An ninh thông tin: Là việc đảm bảo thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước và quyền, lợi ích hợp pháp của tổ chức, cá nhân.

An ninh mạng: Là trạng thái hoạt động trên không gian mạng mà không gây phương hại, ảnh hưởng đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

Rủi ro an toàn thông tin: Là khả năng xảy ra các tác động chủ quan hoặc khách quan làm ảnh hưởng đến trạng thái an toàn của thông tin mạng.

Sự cố an toàn thông tin mạng: Là tình huống thông tin hoặc hệ thống thông tin bị xâm phạm, gây mất toàn vẹn, mất bảo mật hoặc gián đoạn khả năng sử dụng.

Hệ thống thông tin của cơ quan, đơn vị: Là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập để phục vụ hoạt động tạo lập, xử lý, lưu trữ, truyền đưa và chia sẻ thông tin trên mạng.

Hệ thống thông tin quan trọng: Là hệ thống thông tin có vai trò thiết yếu đối với hoạt động chỉ đạo, điều hành, bảo mật hoặc phục vụ trực tiếp công tác nghiệp vụ của cơ quan, đơn vị. Bao gồm:

+ Hạ tầng mạng (thiết bị, hệ thống kết nối, đường truyền, thiết bị phụ trợ);

+ Hệ thống xử lý, lưu trữ dữ liệu nghiệp vụ.

Chủ quản hệ thống thông tin: Là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin.

Đơn vị vận hành hệ thống thông tin: Là cơ quan, đơn vị được chủ quản hệ thống thông tin giao nhiệm vụ vận hành hệ thống thông tin. Trong trường hợp chủ quản hệ thống thông tin thuê ngoài dịch vụ công nghệ thông tin, đơn vị vận hành hệ thống thông tin là bên cung cấp dịch vụ.

Bộ phận chuyên trách về an toàn thông tin: Là bộ phận do chủ quản hệ thống thông tin thành lập hoặc chỉ định để thực thi nhiệm vụ bảo đảm an toàn thông tin và ứng cứu sự cố an toàn thông tin mạng.

Tài sản công nghệ thông tin: Các trang thiết bị, thông tin thuộc hệ thống công nghệ thông tin của đơn vị, bao gồm:

- Phần cứng: là sản phẩm thiết bị số hoàn chỉnh; cụm linh kiện; linh kiện; bộ phận của thiết bị số, cụm linh kiện, linh kiện.

- Phần mềm: là chương trình máy tính được mô tả bằng hệ thống ký hiệu, mã hoặc ngôn ngữ để điều khiển thiết bị số thực hiện chức năng nhất định.

- Thông tin: là tin, dữ liệu được chứa đựng trong văn bản, hồ sơ, tài liệu có sẵn, tồn tại dưới dạng bản viết, bản in, bản điện tử, tranh, ảnh, bản vẽ, băng, đĩa, bản ghi hình, ghi âm hoặc các dạng khác do cơ quan nhà nước, đơn vị tạo ra.

- Dữ liệu: là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự.

Dữ liệu quan trọng (Important Data): Là dữ liệu được đơn vị xác định cần ưu tiên bảo vệ, bao gồm nhưng không giới hạn: thông tin nghiệp vụ, thông tin bí mật nhà nước, thông tin cá nhân và các loại thông tin quan trọng khác (nếu có).

Giám sát hệ thống thông tin (Information System Monitoring): Là việc theo dõi trạng thái hoạt động của hệ thống thông tin để phát hiện sự cố, bất thường.

Nhật ký hệ thống (System Log): Là bản ghi tự động lưu lại các sự kiện liên quan đến hoạt động, an ninh hoặc thao tác chỉnh sửa dữ liệu trên hệ thống như: sao chép, sửa đổi, xoá bỏ thông tin lưu trữ trong thông tin.

Phương tiện lưu trữ (media Storage): Là các thiết bị, phương tiện được sử dụng để lưu trữ, sao chép, trao đổi thông tin giữa các thiết bị, máy tính một cách gián tiếp.

Điều 3. Nguyên tắc bảo đảm an toàn thông tin, an ninh mạng

- Đảm bảo hệ thống mạng nội bộ an toàn, ổn định.

- Tuân thủ luật pháp Việt Nam và tuân thủ theo Điều 4 Luật An toàn thông tin mạng, Điều 4 Luật An ninh mạng và các quy định pháp luật khác có liên quan.

- Ngăn ngừa truy cập trái phép, bảo vệ dữ liệu nội bộ, và duy trì khả năng phản ứng sự cố.

- Không truy cập các trang web không rõ nguồn gốc.

- Không tải hoặc cài đặt phần mềm không rõ nguồn gốc.

- Việc truy cập mạng phục vụ mục đích công việc là chính, hạn chế sử dụng cho mục đích cá nhân.

- Máy tính cần có phần mềm diệt virus được cập nhật thường xuyên.

- Mọi hành vi cố ý xâm nhập trái phép, gây mất an toàn thông tin, an ninh mạng sẽ bị xử lý kỷ luật hoặc truy cứu trách nhiệm theo pháp luật.

- Trường hợp có văn bản quy định cập nhật, thay thế hoặc quy định khác tại văn bản quy phạm pháp luật, quyết định của cấp có thẩm quyền cao hơn thì áp dụng quy định tại văn bản đó.

Điều 4. Các hành vi bị nghiêm cấm

Các hành vi bị nghiêm cấm về an toàn thông tin được quy định tại:

- Điều 7 Luật An toàn thông tin mạng; Điều 8 Luật An ninh mạng.

- Xâm nhập trái phép vào hệ thống thông tin.

- Truy cập trái phép vào phần mềm.

- Tự ý xóa bỏ, tháo gỡ hoặc thay đổi thông số thiết lập của phần mềm, gây ảnh hưởng đến việc vận hành hệ thống.

- Truy cập, sử dụng trái phép thông tin mật.

- Lợi dụng phần mềm hoặc dữ liệu của phần mềm vào các mục đích không thuộc phạm vi, chức năng, nhiệm vụ được phân công.

- Cung cấp, phát tán thông tin, dữ liệu trái với quy định của đơn vị.

- Gây mất an toàn thông tin, an ninh mạng.

- Cung cấp, phát tán thông tin trái phép, làm ảnh hưởng đến hệ thống.

- Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ IP, thiết bị phát sóng như điểm truy cập mạng không dây của cá nhân vào mạng nội bộ mà không có sự hướng dẫn hoặc đồng ý của đơn vị quản lý, vận hành hệ thống mạng nội bộ.

CHƯƠNG II: QUY ĐỊNH CHUNG VỀ AN TOÀN THÔNG TIN (ATTT), AN NINH MẠNG (ANM)

Điều 5. Mục đích

- Đảm bảo hệ thống mạng nội bộ an toàn, ổn định, hiệu suất cao.

- Tuân thủ luật pháp Việt Nam và các tiêu chuẩn quốc tế (ISO 27001, NIST nếu có).

- Ngăn ngừa truy cập trái phép, bảo vệ dữ liệu nội bộ, và duy trì khả năng phản ứng khi xảy ra sự cố.

Điều 6. Bảo vệ hệ thống mạng nội bộ và Internet

- Hệ thống mạng nội bộ phải được bảo vệ bằng tường lửa, kiểm soát truy cập và có cơ chế mã hóa dữ liệu.

- Tất cả các hệ thống máy chủ, máy trạm, ứng dụng phải được cài đặt phần mềm phòng chống mã độc và phần mềm diệt virus.

- Hệ thống mạng nội bộ tối thiểu được phân thành các vùng:

+ Vùng mạng biên: Được đặt các thiết bị Router, Firewall để kết nối hệ thống ra các mạng bên ngoài và mạng Internet;

+ Mạng WAN (Wide Area Network), hay mạng diện rộng, là một mạng máy tính kết nối các mạng cục bộ (LAN) và các mạng khác;

+ Vùng mạng nội bộ: (LAN - local area network hay users zone) là vùng mạng được thiết lập để cung cấp kết nối mạng cho các máy trạm và các thiết bị đầu cuối và các thiết bị khác của người sử dụng vào hệ thống;

+ Vùng mạng không dây: Cung cấp các kết nối mạng không dây cho các thiết bị của người dùng vào hệ thống.

- Đối với các phần mềm nghiệp vụ của đơn vị, yêu cầu thực hiện các nội dung sau:

+ Các log hệ thống được lưu trữ tối thiểu 03 tháng.

+ Có phương án sao lưu dữ liệu định kỳ, kiểm tra phục hồi mỗi quý.

+ Có kế hoạch phản ứng sự cố (Incident Response Plan) để đảm bảo khả năng phục hồi khi xảy ra sự cố.

+ Giám sát thường xuyên và liên tục để phát hiện, cảnh báo sớm các nguy cơ mất an toàn thông tin.

Điều 7. Đối với phòng máy chủ

- Phân công đầu mối chịu trách nhiệm đảm bảo an toàn, an ninh thông tin.

- Xây dựng nội quy làm việc tại phòng máy chủ; phân công cán bộ giám sát hệ thống CNTT; có sổ nhật ký ghi nhận ra vào.

- Đề xuất phương án đảm bảo lưu điện, sử dụng máy phát điện đủ công suất để duy trì hoạt động của phòng máy chủ ít nhất 3 tiếng khi mất điện lưới.

Điều 8. Quy định về tài khoản và mật khẩu

- Mật khẩu phải có ít nhất 8 ký tự, bao gồm chữ cái, số và ký tự đặc biệt.

- Định kỳ thay đổi mật khẩu (90 ngày đối với tài khoản người dùng).

- Không chia sẻ mật khẩu, phải thay đổi ngay khi nghi ngờ bị lộ.

- Nếu không thể đổi mật khẩu, phải làm thủ tục đặt lại mật khẩu theo quy trình tại phụ lục 1 kèm theo.

- Khi người dùng thay đổi vị trí công tác, nghỉ việc hoặc nghỉ hưu, đơn vị phải thu hồi tất cả các tài khoản truy cập vào các hệ thống thông tin và báo cho bộ phận quản trị mạng để hủy bỏ quyền truy cập.

CHƯƠNG III: PHƯƠNG ÁN PHÒNG NGỪA RỦI RO VÀ XỬ LÝ SỰ CỐ AN TOÀN THÔNG TIN, AN NINH MẠNG

Điều 9. Phương án phòng ngừa rủi ro và xử lý xự cố an toàn thông tin, an ninh mạng

- Bộ phận quản trị mạng phải thiết lập và vận hành hệ thống giám sát an ninh mạng nhằm theo dõi, phát hiện và ngăn chặn các mối đe dọa về an toàn thông tin.

- Hệ thống giám sát cần hoạt động ổn định, liên tục; ghi nhật ký truy cập hàng ngày và đảm bảo bảo mật dữ liệu trong toàn bộ quá trình theo dõi.

- Thực hiện giám sát định kỳ; phối hợp với đơn vị chức năng để phân tích, đánh giá, thống kê kết quả xử lý sự cố phục vụ công tác quản lý và báo cáo.

- Nhận diện các nguy cơ tiềm ẩn như:

+ Tấn công mạng (DDoS, Phishing, Malware, Ransomware…).

+ Lỗ hổng bảo mật trong phần mềm, hệ thống.

+ Rò rỉ dữ liệu do truy cập trái phép hoặc cấu hình sai.

- Đánh giá mức độ ảnh hưởng và áp dụng các biện pháp phòng ngừa phù hợp:

+ Sử dụng hệ thống tường lửa (Firewall) và thiết bị/phần mềm phát hiện, ngăn chặn xâm nhập (IDS/IPS).

+ Thực hiện phân vùng mạng (network segmentation) để hạn chế tác động khi xảy ra sự cố.

+ Áp dụng xác thực truy cập, giới hạn quyền người dùng theo nguyên tắc tối thiểu.

+ Bảo vệ thiết bị đầu cuối, đặc biệt trước các loại mã độc.

+ Sao lưu dữ liệu định kỳ; áp dụng mã hóa cho dữ liệu quan trọng.

+ Kiểm soát chặt chẽ việc truyền tải và xuất dữ liệu ra bên ngoài.

+ Xây dựng kế hoạch khôi phục sau sự cố và đảm bảo khả năng phục hồi hệ thống.

- Khi phát hiện sự cố an toàn thông tin hoặc an ninh mạng, cá nhân hoặc đơn vị liên quan phải báo cáo ngay lập tức đến bộ phận chuyên trách về an ninh mạng. Đồng thời thực hiện ghi nhận đầy đủ thông tin về sự cố; tiến hành điều tra nguyên nhân, đánh giá phạm vi ảnh hưởng; triển khai các biện pháp kỹ thuật, nghiệp vụ để khắc phục hậu quả, khôi phục trạng thái an toàn của hệ thống.

- Phối hợp với cơ quan chức năng hoặc đối tác hỗ trợ điều tra nếu cần thiết.

- Cập nhật các quy trình phòng ngừa; bổ sung các biện pháp kiểm soát mới để giảm thiểu khả năng tái diễn sự cố.

- Tổ chức diễn tập ứng phó sự cố định kỳ nhằm nâng cao năng lực phản ứng, khả năng phối hợp và cải tiến quy trình xử lý tình huống thực tế.

CHƯƠNG IV: TRÁCH NHIỆM BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN

Điều 10. Trách nhiệm của đơn vị quản lý và chủ quản hệ thống thông tin

- Thiết kế, triển khai và vận hành hạ tầng công nghệ thông tin (bao gồm: mạng nội bộ, máy chủ, hệ thống lưu trữ, phần mềm, thiết bị đầu cuối...).

- Theo dõi, kiểm soát hoạt động hệ thống để bảo đảm tính ổn định, liên tục và hiệu suất cao.

- Lập kế hoạch và thực hiện sao lưu dữ liệu định kỳ; phục hồi khi xảy ra sự cố.

- Áp dụng các biện pháp bảo mật như: tường lửa, phần mềm chống virus, mã hóa dữ liệu, xác thực đa yếu tố.

- Kiểm tra định kỳ tình trạng hệ thống, thiết bị và phần mềm; báo cáo kết quả vận hành, sự cố (nếu có), đồng thời đề xuất phương án nâng cấp, cải tiến hệ thống gửi cấp có thẩm quyền.

- Hướng dẫn cán bộ, nhân viên sử dụng hệ thống phần mềm đúng quy trình; hỗ trợ kỹ thuật khi xảy ra lỗi phần mềm hoặc sự cố hệ thống.

- Đảm bảo các hệ thống thông tin tuân thủ Kiến trúc Chính phủ điện tử của Bộ Xây dựng và Cục Hàng không Việt Nam; thực hiện đánh giá cấp độ theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ.

- Xây dựng các quy chế, chính sách bảo mật, quy định cho các hệ thống thông tin phù hợp với quy định hiện hành.

- Giám sát an toàn thông tin, an ninh mạng theo quy định, bao gồm cả các quy định tại Điều 20 Nghị định số 85/2016/NĐ-CP.

- Phát hiện và xử lý kịp thời các hành vi truy cập trái phép, tấn công mạng, rò rỉ thông tin; thực hiện biện pháp thu hồi hoặc khóa quyền truy cập của tài khoản vi phạm.

- Cử cá nhân hoặc bộ phận chuyên trách làm đầu mối giám sát, cảnh báo và phối hợp với cơ quan chức năng trong công tác bảo đảm an toàn thông tin.

- Chịu trách nhiệm về tính sẵn sàng, độ tin cậy, bảo mật và tuân thủ pháp luật của hệ thống thông tin, đặc biệt trong trường hợp xảy ra sự cố nghiêm trọng.

Điều 11. Trách nhiệm của cán bộ, công chức, viên chức và người lao động khi sử dụng mạng nội bộ

- Tuân thủ các quy định, chính sách nội bộ của cơ quan, đơn vị; chấp hành nghiêm các quy định về sử dụng mạng nội bộ đã được ban hành.

- Không chia sẻ tài khoản truy cập hoặc mật khẩu cho người khác.

- Tự bảo vệ thông tin cá nhân, thông tin công việc và dữ liệu quan trọng trong quá trình sử dụng mạng.

- Không tải, lưu trữ hoặc phát tán các tập tin độc hại, phần mềm gián điệp hoặc dữ liệu không rõ nguồn gốc.

- Chỉ sử dụng mạng nội bộ vào mục đích công việc; không sử dụng cho các hoạt động cá nhân không liên quan.

- Không truy cập hoặc truyền tải nội dung vi phạm pháp luật, phản cảm, mang tính chính trị không phù hợp hoặc có tính chất kích động.

- Không tự ý cài đặt, chỉnh sửa hoặc gỡ bỏ phần mềm, ứng dụng trong hệ thống khi chưa có sự cho phép của bộ phận kỹ thuật hoặc phụ trách công nghệ thông tin.

- Không kết nối thiết bị cá nhân (USB, ổ cứng di động, thiết bị mạng không dây cá nhân...) vào mạng nội bộ nếu chưa được kiểm tra và xác nhận an toàn.

- Báo cáo ngay với bộ phận quản trị mạng khi phát hiện sự cố, hành vi bất thường hoặc nguy cơ rò rỉ thông tin.

- Hợp tác đầy đủ khi có yêu cầu kiểm tra, đánh giá an toàn thông tin hoặc điều tra sự cố mạng.

- Không thực hiện các hành vi gây ảnh hưởng đến hoạt động ổn định của mạng nội bộ như: phát tán virus, tấn công từ chối dịch vụ (DoS), sử dụng băng thông không đúng mục đích.

- Chịu trách nhiệm hoàn toàn trước pháp luật và tổ chức đối với hành vi vi phạm trong quá trình sử dụng mạng nội bộ.

- Trong trường hợp gây thiệt hại, cá nhân vi phạm có thể bị xử lý hành chính, kỷ luật hoặc truy cứu trách nhiệm hình sự tùy theo mức độ vi phạm.

- Khi nghỉ việc, luân chuyển công tác hoặc thay đổi máy trạm, người sử dụng phải bàn giao đầy đủ thiết bị, dữ liệu và tài khoản truy cập theo quy định.

Điều 12. Trách nhiệm của Văn phòng Cục Hàng Không Việt Nam

- Quản lý việc ra vào phòng máy chủ và yêu cầu ghi nhận đầy đủ vào nhật ký truy cập.

- Xây dựng nội quy làm việc trong khu vực phòng máy chủ và phân công cán bộ giám sát thường xuyên.

- Duy trì hệ thống lưu điện, đảm bảo vận hành ít nhất 3 giờ sau khi xảy ra sự cố mất điện.

- Áp dụng các biện pháp kiểm soát truy nhập nhằm bảo vệ thiết bị kết nối mạng và các hệ thống bảo mật quan trọng, bao gồm: tường lửa, thiết bị định tuyến và hệ thống lưu trữ.

- Thực hiện các biện pháp bảo đảm an toàn, an ninh cho hệ thống theo Điều 6 và Điều 7 của Quy chế này.

- Phối hợp chặt chẽ với đơn vị vận hành hệ thống thông tin để đảm bảo an toàn trong mọi giai đoạn hoạt động.

- Bảo vệ các hệ thống thông tin và cơ sở dữ liệu quan trọng của Cục Hàng không Việt Nam.

- Khi xảy ra sự cố về an toàn thông tin, phải kịp thời báo cáo cho Trung tâm Ứng cứu khẩn cấp (Trung tâm Công nghệ thông tin, Bộ Xây dựng) để được hỗ trợ.

- Lập kế hoạch ngân sách, đầu tư hoặc thuê: Phần mềm phát hiện, diệt Virus cho các máy tính được Cục Hàng không Việt Nam trang bị; Phần cứng và phần mềm chuyên dụng để bảo vệ ngăn chặn các hành vi can thiệp bất hợp pháp từ xa đối với các phần mềm nghiệp vụ của Cục Hàng không Việt Nam.

Điều 13. Trách nhiệm của Phòng Khoa học, Công nghệ và Môi trường

- Là đơn vị chuyên trách về An toàn thông tin, an ninh mạng của Cục Hàng không Việt Nam.

- Chủ trì, phối hợp với các đơn vị thuộc Cục Hàng không Việt Nam tham gia diễn tập ứng cứu sự cố an toàn thông tin theo kế hoạch của Bộ Xây dựng.

- Tham gia các cuộc diễn tập về an toàn thông tin do cơ quan điều phối quốc gia hoặc các tổ chức quốc tế tổ chức.

- Phối hợp với các đơn vị liên quan tổ chức tập huấn, bồi dưỡng nâng cao kiến thức, kỹ năng về an toàn, an ninh mạng cho công chức, viên chức và người lao động.

- Hướng dẫn, giám sát, đôn đốc việc triển khai thực hiện Quy chế và các quy định liên quan.

- Hỗ trợ các đơn vị trong công tác bảo đảm an toàn thông tin và an ninh mạng.

- Chủ trì, phối hợp với các đơn vị liên quan xây dựng kế hoạch, báo cáo về an toàn thông tin và an ninh mạng của Cục Hàng không Việt Nam.

- Theo dõi, tổng hợp tình hình thực hiện công tác an toàn thông tin, an ninh mạng tại các đơn vị; định kỳ báo cáo lãnh đạo Cục và Bộ Xây dựng theo quy định.

- Lập kế hoạch kiểm tra hằng năm việc thực hiện Quy chế tại các đơn vị.

- Mời các đơn vị chuyên trách về an ninh, an toàn mạng thông tin của Bộ Công an kiểm tra, phát hiện lỗ hổng trong sử dụng mạng máy tính nội bộ, mạng máy tính có kết nối Internet để kịp thời phòng ngừa, khắc phục.

- Chủ trì, phối hợp xử lý các khó khăn, vướng mắc phát sinh trong quá trình triển khai thực hiện Quy chế.

Điều 14. Trách nhiệm của các đơn vị thuộc Cục Hàng không Việt Nam

- Tổ chức triển khai thực hiện nghiêm túc Quy chế này tại đơn vị mình.

- Phổ biến, quán triệt đến toàn thể cán bộ, công chức, viên chức và người lao động các nội dung, quy định trong Quy chế.

- Trong quá trình thực hiện, nếu phát sinh khó khăn, vướng mắc, đơn vị có trách nhiệm phản ánh kịp thời về Phòng Khoa học, Công nghệ và Môi trường để tổng hợp, báo cáo Cục trưởng xem xét, sửa đổi hoặc bổ sung kịp thời.

Điều 15. Trách nhiệm của đơn vị và bên thứ ba trong việc cung cấp, sử dụng sản phẩm, dịch vụ công nghệ thông tin

Việc cung cấp, sử dụng sản phẩm, dịch vụ công nghệ thông tin giữa đơn vị và bên thứ ba phải bảo đảm các yêu cầu về an toàn thông tin, an ninh mạng và tuân thủ quy định pháp luật. Các bên có trách nhiệm thực hiện các nội dung sau:

1. Trách nhiệm của đơn vị sử dụng dịch vụ

- Tuân thủ các quy định của pháp luật và nội bộ về an toàn, an ninh mạng trong quá trình hợp tác với bên thứ ba.

- Xác lập, thông báo rõ ràng các yêu cầu về bảo mật, quyền truy cập, phạm vi sử dụng đối với sản phẩm, dịch vụ công nghệ thông tin.

- Yêu cầu bên thứ ba thực hiện đầy đủ các biện pháp bảo đảm an toàn thông tin.

- Kiểm soát chặt chẽ quyền truy cập của bên thứ ba vào hệ thống thông tin; thu hồi quyền truy cập, thay đổi khóa bảo mật ngay sau khi hoàn thành công việc hoặc chấm dứt hợp đồng.

- Theo dõi nhân sự bên thứ ba trong quá trình triển khai; phát hiện vi phạm phải kịp thời thông báo và phối hợp xử lý.

- Bảo đảm các nghĩa vụ bàn giao, kiểm thử, nghiệm thu sản phẩm, dịch vụ diễn ra theo đúng quy định.

2. Trách nhiệm của bên thứ ba cung cấp dịch vụ

- Xây dựng kế hoạch triển khai hợp đồng; bố trí nhân sự và nguồn lực phù hợp.

- Cung cấp danh sách nhân sự tham gia triển khai cho đơn vị sử dụng để xem xét, phê duyệt.

- Đảm bảo toàn bộ nhân sự tham gia dự án ký và tuân thủ cam kết bảo mật trong suốt quá trình thực hiện và sau khi kết thúc hợp đồng.

- Thực hiện kiểm tra, đánh giá an toàn thông tin và an ninh mạng đối với sản phẩm, dịch vụ được cung cấp.

- Tiến hành kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng chính thức.

- Bàn giao đầy đủ tài sản, tài liệu, mã nguồn (nếu có) và quyền truy cập vào hệ thống theo hợp đồng khi hoàn tất công việc hoặc kết thúc hợp đồng.

Chương VI: CHẾ ĐỘ BÁO CÁO

Điều 16. Chế độ báo cáo

Tất cả các cơ quan, đơn vị có trách nhiệm gửi báo cáo về Cục Hàng không Việt Nam (qua Phòng Khoa học, Công nghệ và Môi trường) theo các hình thức sau:

1. Báo cáo định kỳ hằng năm

a) Nội dung báo cáo: Theo biểu mẫu báo cáo tại phụ lục 2

b) Thời hạn gửi báo cáo: Trước ngày 31/01 hằng năm.

2. Báo cáo đột xuất

a) Trường hợp xảy ra sự cố an toàn thông tin, an ninh mạng:

Thời hạn gửi: Trong vòng 03 (ba) ngày làm việc kể từ thời điểm phát hiện sự cố;

Nội dung báo cáo theo biểu mẫu báo cáo tại phụ lục 3.

b) Các trường hợp phát sinh khác: Thực hiện theo yêu cầu đột xuất của Cục Hàng không Việt Nam.

Phụ Lục 1

QUY TRÌNH THIẾT LẬP VÀ THAY ĐỔI MẬT KHẨU

1. Quản lý tài khoản truy cập

Đơn vị quản lý vận hành các hệ thống thông tin có trách nhiệm:

Tạo lập, cung cấp, phân quyền, tạm dừng và thu hồi tài khoản truy cập cho cán bộ, công chức, viên chức theo đề xuất của các đơn vị hoặc theo quy chế quản trị.

Xử lý các yêu cầu hỗ trợ tài khoản trong vòng 24 giờ làm việc kể từ khi tiếp nhận yêu cầu.

2. Sử dụng tài khoản truy cập

Người dùng có trách nhiệm:

Đăng nhập bằng tài khoản được cấp, thay đổi mật khẩu trong lần đầu tiên và định kỳ 90 ngày/lần.

Sử dụng mật khẩu mạnh (tối thiểu 8 ký tự, bao gồm chữ hoa, chữ thường, số và ký tự đặc biệt).

Không chia sẻ thông tin đăng nhập.

Đăng xuất khỏi hệ thống sau khi sử dụng.

Khi nghi ngờ lộ mật khẩu, phải tự thay mật khẩu hoặc liên hệ bộ phận quản trị để hỗ trợ.

3. Quản lý mật khẩu truy cập

3.1. Tạo mật khẩu lần đầu

Mật khẩu tạm thời được cung cấp bởi Bộ phận quản trị mạng.

Người dùng phải đổi mật khẩu ngay lần đăng nhập đầu tiên.

Mật khẩu mới phải đáp ứng yêu cầu độ mạnh như trên.

Ví dụ: Hkvn@2025

3.2. Thay đổi mật khẩu định kỳ

Thực hiện đổi mật khẩu mỗi 90 ngày/lần.

Tuyệt đối không chia sẻ mật khẩu.

Khi nghi ngờ bị lộ mật khẩu:

Người dùng thay đổi mật khẩu ngay;

Nếu không thể đổi, liên hệ bộ phận quản trị để được hỗ trợ.

4. Quy trình cấp lại mật khẩu

Người dùng lập văn bản đề nghị cấp lại mật khẩu.

Trưởng đơn vị (lãnh đạo phòng, ban) phê duyệt.

Văn bản chuyển đến Bộ phận quản trị mạng để xử lý.

Người dùng được cung cấp mật khẩu tạm thời và phải đổi lại ngay khi đăng nhập.

5. Thu hồi và vô hiệu hóa tài khoản

Áp dụng trong các trường hợp: nghỉ việc, nghỉ hưu, luân chuyển, thôi nhiệm vụ.

Đơn vị trực tiếp quản lý phải thông báo ngay cho bộ phận quản trị mạng.

Bộ phận quản trị thực hiện vô hiệu hóa tài khoản tạm thời hoặc vĩnh viễn tùy theo yêu cầu.

Phụ Lục 2

Biểu mẫu báo cáo định kỳ

BÁO CÁO KẾT QUẢ THỰC HIỆN QUY CHẾ SỬ DỤNG MẠNG MÁY TÍNH NỘI BỘ, MẠNG MÁY TÍNH CÓ KẾT NỐI INTERNET

I. Thông tin đơn vị

Tên đơn vị: ……

Người phụ trách công nghệ thông tin: ……

Số điện thoại và địa chỉ email liên hệ: ……

II. Kết quả thực hiện công tác bảo đảm an toàn, an ninh mạng

1. Hiện trạng hệ thống thông tin

Đơn vị đang quản lý, vận hành bao nhiêu hệ thống thông tin? Tên và chức năng cụ thể của từng hệ thống?

Có bao nhiêu hệ thống đã được phê duyệt cấp độ an toàn thông tin theo Nghị định 85/2016/NĐ-CP? Thuộc cấp độ mấy?

Những hệ thống nào chưa được phê duyệt? Hiện đang trong quá trình đề xuất cấp độ hay chưa?

2. Hạ tầng mạng – Thiết bị

Các giải pháp đã triển khai để đảm bảo an toàn thông tin và an ninh mạng?

Đơn vị có hệ thống giám sát 24/7 hoặc quy trình phát hiện, ứng phó sự cố không?

Các biện pháp đang áp dụng để bảo vệ thiết bị đầu cuối, máy chủ và ngăn chặn truy cập trái phép?

Tổng số máy tính hiện có; số máy đã được cài đặt phần mềm diệt virus và cập nhật thường xuyên?

Các máy tính có được cài đặt hệ điều hành và phần mềm bản quyền (Windows, Office...) không? Có cập nhật phần mềm định kỳ không? Tần suất cập nhật?

3. Bảo mật tài khoản người dùng

Tổng số tài khoản đang hoạt động: …….

Trong năm có bao nhiêu sự thay đổi về tài khoản (cấp mới, thu hồi, thay đổi quyền)?

4. Giám sát và xử lý sự cố.

Trong tháng/quý/năm có phát hiện hành vi xâm nhập trái phép hoặc tấn công mạng nào không?

Có hành động xử lý, báo cáo, phục hồi sau sự cố không? (Nếu có, ghi rõ)

5. Tổng kết kết quả thực hiện Quy chế.

Đánh giá chung việc thực hiện công tác an toàn thông tin và an ninh mạng theo Quy chế được ban hành.

III. Kiến nghị, đề xuất.

Những khó khăn, vướng mắc trong quá trình thực hiện.

Nhu cầu hỗ trợ từ các cấp (kinh phí, đào tạo, giải pháp kỹ thuật…).

Kiến nghị cụ thể để nâng cao hiệu quả công tác bảo đảm an toàn, an ninh mạng.

Phụ Lục 3

Biểu mẫu báo cáo đột xuất

(Áp dụng trong trường hợp xảy ra sự cố an toàn thông tin hoặc an ninh mạng)

I. Thông tin đơn vị

Tên đơn vị: ……

Người phụ trách CNTT: ……

Số điện thoại và địa chỉ email liên hệ: ……

II. Nội dung báo cáo

1. Mô tả sự cố:

Loại sự cố (tấn công mạng, rò rỉ dữ liệu, mất quyền truy cập…)

Mô tả ngắn gọn diễn biến vụ việc

2. Thời gian và địa điểm xảy ra

Ngày, giờ

Hệ thống/địa điểm cụ thể

3. Nguyên nhân (nếu xác định được)

Lỗi người dùng / lỗi hệ thống / phần mềm độc hại…

4. Đánh giá rủi ro và ảnh hưởng

Mức độ rủi ro: thấp / trung bình / cao

Ảnh hưởng đến: hệ thống kỹ thuật, dữ liệu, hoạt động nghiệp vụ…

5. Biện pháp xử lý và khắc phục

Hành động đã thực hiện

Còn tiếp diễn hoặc đã khôi phục hoàn toàn?

6. Kiến nghị (nếu có)

Hỗ trợ kỹ thuật

Điều chỉnh quy trình

Bổ sung nhân lực / công cụ…