|  |  |
| --- | --- |
| BỘ GIAO THÔNG VẬN TẢI**CỤC HÀNG KHÔNG VIỆT NAM** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM****Độc lập - Tự do - Hạnh phúc** |
| Số: /QĐ-CHK | *Hà Nội, ngày tháng năm 2017* |

**QUYẾT ĐỊNH**

**Ban hành Quy chế bảo đảm an toàn, an ninh mạng thông tin**

**trong lĩnh vực Hàng không dân dụng**

**CỤC TRƯỞNG CỤC HÀNG KHÔNG VIỆT NAM**

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015;

Căn cứ Luật Công nghệ thông tin số 67/2006/QH11 ngày 29/6/2006;

Căn cứ Luật Giao dịch điện tử số 51/2005/QH11 ngày 29/11/2005;

Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông Quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Quyết định số 121/QĐ-BGTVT Ngày 14/01/2016, của Bộ trưởng Bộ GTVT quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Cục HKVN;

Xét đề nghị của Trưởng phòng Khoa học công nghệ và môi trường,

**QUYẾT ĐỊNH**

**Điều 1**: Ban hành kèm theo Quyết định này Quy chếbảo đảm an toàn, an ninh mạng thông tin trong lĩnh vực Hàng không dân dụng.

**Điều 2**: Quyết định này có hiệu lực từ ngày ký.

**Điều 3**: Chánh Văn phòng, Thủ trưởng các cơ quan, đơn vị ngành Hàng không Việt Nam chịu trách nhiệm thi hành Quyết định này./.

|  |  |
| --- | --- |
|  |  **CỤC TRƯỞNG** |
| ***Nơi nhận:***- Như điều 3- TT CNTT Bộ GTVT (để b/c);- Các Phó Cục trưởng;- Lưu: VT, KHCNMT. |  |

|  |  |
| --- | --- |
| BỘ GIAO THÔNG VẬN TẢI**CỤC HÀNG KHÔNG VIỆT NAM** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM****Độc lập - Tự do - Hạnh phúc** |

**QUY CHẾ BẢO ĐẢM AN TOÀN, AN NINH THÔNG TIN MẠNG TRONG LĨNH VỰC HÀNG KHÔNG DÂN DỤNG**

**Chương I: QUY ĐỊNH CHUNG**

**Điều 1. Nguyên tắc chung.**

Nhằm đảm bảo an toàn, an ninh thông tin trong lĩnh vực Hàng không dân dụng cụ thể như sau:

1. Nguyên tắc bảo đảm an toàn thông tin phải tuân thủ các nguyên tắc tại Điều 4 của Luật An toàn thông tin và Điều 4 của Nghị định số 85/2016/NĐ-CP;

2. Tất cả các cơ quan, đơn vị trong ngành Hàng không có trách nhiệm bảo đảm an toàn thông tin của cơ quan, đơn vị mình theo đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước;

3. Được thực hiện thường xuyên, liên tục từ khâu thiết kế, xây dựng, vận hành đến khi hủy bỏ; tuân thủ theo các tiêu chuẩn, quy chuẩn kỹ thuật được các cơ quan chức năng ban hành;

4. Nhận biết, phân loại, đánh giá kịp thời và xử lý có hiệu quả các rủi ro an toàn thông tin mạng có thể xảy ra trong cơ quan, đơn vị;

5. Xây dựng, triển khai quy chế an toàn thông tin trên cơ sở hài hòa giữa lợi ích, chi phí và mức độ chấp nhận rủi ro của đơn vị;

6. Bố trí nhân sự chuyên trách chịu trách nhiệm bảo đảm an toàn thông tin.

7. Xác định rõ quyền hạn, trách nhiệm của Thủ trưởng cơ quan, đơn vị (hoặc người đại diện hợp pháp), từng bộ phận và cá nhân trong cơ quan, đơn vị đối với công tác bảo đảm an toàn thông tin mạng.

**Điều 2. Phạm vi, đối tượng áp dụng.**

1. Phạm vi áp dụng.

Quy chế này được áp dụng đối với tất cả các cơ quan, đơn vị trong ngành Hàng không dân dụng.

2. Đối tượng áp dụng.

Cán bộ, công chức, viên chức, nhân viên đang làm việc trong các cơ quan, đơn vị trong lĩnh vực Hàng không dân dụng.

**Điều 3. Giải thích từ ngữ.**

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

1. Trung tâm dữ liệu bao gồm hạ tầng kỹ thuật (nhà trạm, hệ thống cáp) và hệ thống máy tính cùng các thiết bị phụ trợ được lắp đặt vào đó để lưu trữ, trao đổi và quản lý tập trung dữ liệu của một hay nhiều tổ chức, cá nhân;

2. Thiết bị di động là thiết bị số có thể cầm tay, có hệ điều hành, có khả năng xử lý, kết nối mạng và có màn hình hiển thị như máy tính xách tay, máy tính bảng, điện thoại di động thông minh;

3. Vật mang tin là các phương tiện vật chất dùng để lưu giữ và truyền nhận thông tin điện tử;

4. Rủi ro an toàn thông tin là những nhân tố chủ quan hoặc khách quan có khả năng ảnh hưởng đến trạng thái an toàn thông tin mạng;

5. Dữ liệu nhạy cảm là dữ liệu có thông tin mật, thông tin lưu hành nội bộ của đơn vị hoặc do đơn vị quản lý, nếu lộ lọt ra ngoài sẽ gây ảnh hưởng xấu đến danh tiếng, tài chính và hoạt động của đơn vị;

6. Tài khoản người dùng là một tập hợp thông tin đại diện duy nhất cho người sử dụng trên hệ thống thông tin, người dùng sử dụng để đăng nhập và truy cập các tài nguyên được cấp phép trên hệ thống thông tin đó. Tài khoản người dùng ít nhất phải bao gồm tên định danh và mã khóa bí mật;

7. Bên thứ ba là các tổ chức, cá nhân được đơn vị thuê hoặc hợp tác với đơn vị nhằm cung cấp hàng hóa, dịch vụ kỹ thuật cho hệ thống thông tin;

8. Tường lửa là tập hợp các thành phần hoặc một hệ thống các trang thiết bị, phần mềm được đặt giữa hai mạng, nhằm kiểm soát tất cả các kết nối từ bên trong ra bên ngoài mạng hoặc ngược lại;

9. Phần mềm độc hại (mã độc) là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin;

10. Điểm yếu về mặt kỹ thuật là vị trí trong hệ thống thông tin dễ bị khai thác, lợi dụng khi bị tấn công hoặc xâm nhập bất hợp pháp;

11. Tính bảo mật của thông tin là đảm bảo thông tin chỉ được tiếp cận bởi những người được cấp quyền tương ứng;

12. Tính toàn vẹn của thông tin là bảo vệ sự chính xác và đầy đủ của thông tin và thông tin chỉ được thay đổi bởi những người được cấp quyền;

13. Tính sẵn sàng của thông tin là đảm bảo những người được cấp quyền có thể truy xuất thông tin ngay khi có nhu cầu;

14. Sự cố an toàn thông tin mạng là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng đến tính toàn vẹn, tính bảo mật và tính khả dụng;

15. Hệ thống thông tin là tập hợp các thiết bị viễn thông, phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng;

16. Hệ thống thông tin quan trọng là hệ thống thông tin khi phát sinh sự cố sẽ làm tổn hại nghiêm trọng đến hoạt động của cơ quan, đơn vị;

17. An toàn thông tin mạng là sự 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 nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin;

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

**Chương II**

**CÁC QUY ĐỊNH VỀ ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG**

**Điều 4. Quản lý tài sản công nghệ thông tin**

Các loại tài sản công nghệ thông tin bao gồm:

1. Tài sản vật lý: các thiết bị công nghệ thông tin, phương tiện truyền thông và các thiết bị phục vụ cho hoạt động của hệ thống thông tin như hệ thống máy chủ, hệ thống tường lửa (firewall), thiết bị định tuyến (router), Switch, modem ADSL , … phải có các biện pháp bảo vệ, ngăn chặn xâm nhập trái phép;

2. Tài sản thông tin: các thông tin, dữ liệu ở dạng số;

3. Tài sản phần mềm: các phần mềm hệ thống, phần mềm tiện ích, cơ sở dữ liệu, chương trình ứng dụng và công cụ phát triển.

**Điều 5. Yêu cầu cơ bản về quản lý tài sản công nghệ thông tin**

1. Lập danh mục tài sản công nghệ thông tin. Thường xuyên cập nhật và quản lý danh mục.

2. Giao, gán trách nhiệm cho cá nhân hoặc tập thể quản lý, sử dụng tài sản.

3. Quy định các quy tắc sử dụng, gìn giữ, bảo vệ tài sản trong các trường hợp như: mang tài sản ra khỏi cơ quan, tài sản liên quan tới dữ liệu nhạy cảm, cài đặt và cấu hình,...

4. Tài sản vật lý có lưu trữ dữ liệu nhạy cảm khi thay đổi mục đích sử dụng hoặc thanh lý, đơn vị phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó đảm bảo không có khả năng phục hồi. Trường hợp không thể tiêu hủy được dữ liệu, đơn vị phải thực hiện biện pháp tiêu hủy cấu phần lưu trữ dữ liệu trên tài sản đó.

**Điều 6. Yêu cầu chung đối với nơi lắp đặt**

1. Có biện pháp bảo vệ, kiểm soát, hạn chế rủi ro xâm nhập trái phép, phòng chống nguy cơ do cháy nổ, thiên tai, thảm họa.

2. Các khu vực có yêu cầu cao về an toàn như khu vực lắp đặt máy chủ, thiết bị lưu trữ, thiết bị an ninh bảo mật, thiết bị truyền thông phải được cách ly với khu vực dùng chung; ban hành nội quy, hướng dẫn làm việc và áp dụng biện pháp kiểm soát ra vào khu vực đó.

**Điều 7. Yêu cầu đối với Phòng máy chủ, Trung tâm dữ liệu**

Ngoài việc đảm bảo yêu cầu tại Điều 6 Quy chế này, Phòng máy chủ, Trung tâm dữ liệu phải đảm bảo các yêu cầu sau:

1. Khu vực lắp đặt thiết bị phải được tránh nắng chiếu rọi trực tiếp, chống thấm dột nước, tránh ngập lụt. Cửa vào ra phải chắc chắn, có khả năng chống cháy, sử dụng khóa an toàn;

2. Khu vực lắp đặt thiết bị của hệ thống thông tin quan trọng phải được bảo vệ, giám sát 24/7;

3. Có tối thiểu một nguồn điện chính và một nguồn dự phòng có khả năng duy trì hoạt động của thiết bị trong thời gian tối thiểu 30 phút;

4. Có hệ thống điều hòa không khí đảm bảo khả năng hoạt động liên tục;

5. Có hệ thống chống sét trực tiếp và lan truyền;

6. Có hệ thống báo cháy và chữa cháy tự động đảm bảo khi chữa cháy không làm hư hỏng thiết bị lắp đặt bên trong;

7. Có hệ thống sàn kỹ thuật hoặc lớp cách ly chống nhiễm điện;

8. Có hệ thống camera giám sát, lưu trữ dữ liệu tối thiểu 100 ngày;

9. Có hệ thống theo dõi, kiểm soát nhiệt độ, độ ẩm;

10. Có sổ ghi nhật ký ra vào.

**Chương III**

**QUẢN LÝ VẬN HÀNH VÀ THÔNG TIN LIÊN LẠC**

**Điều 8. Vai trò, trách nhiệm đảm bảo an toàn, an ninh thông tin mạng của các cơ quan, đơn vị trong lĩnh vực Hàng không dân dụng.**

**1. Vai trò, trách nhiệm của Lãnh đạo các cơ quan, đơn vị**

a. Vai trò: Lãnh đạo các cơ quan, đơn vị có vai trò lãnh đạo cao nhất về an toàn thông tin mạng tại đơn vị.

b. Trách nhiệm: Chịu trách nhiệm cao nhất về ATTT trong cơ quan, đơn vị. Chỉ huy, tổ chức, triển khai, đôn đốc việc thực hiện các chính sách, quy trình, quy định, hưỡng dẫn và các giải pháp kỹ thuật nhằm đảm bảo an toàn, an ninh thông tin mạng của đơn vị mình.

Chỉ huy các cơ quan, đơn vị chịu trách nhiệm toàn diện trước Cục trưởng Cục Hàng không trong công tác đảm bảo an toàn, an ninh thông tin tại cơ quan, đơn vị.

Tổ chức quán triệt cho cán bộ công chức, viên chức, nhân viên trong cơ quan, đơn vị nâng cao ý thức trách nhiệm bảo vệ an toàn, an ninh thông tin mạng.

Phân công nhân sự thực hiện nhiệm vụ an toàn, an ninh thông tin mạng trong cơ quan, đơn vị.

**2. Vai trò, trách nhiệm quản lý vận hành của các cơ quan, đơn vị**

a. Vai trò: Là đầu mối tiếp nhận, phối hợp ứng cứu, xử lý sự cố ATTT, đảm bảo an toàn, an ninh thông tin tại các cơ quan, đơn vị.

b. Trách nhiệm: Hoạt động theo quy định chức năng, nhiệm vụ, quyền hạn an toàn, an ninh thông tin trong cơ quan, đơn vị.

Thường xuyên kiểm tra, đánh giá điểm yếu về an toàn, an ninh thông tin tại đơn vị; tiến hành áp dụng các biện pháp, giải pháp kỹ thuật nhằm đảm bảo ATTT tại cơ quan, đơn vị.

Ban hành các quy trình vận hành hệ thống thông tin, tối thiểu bao gồm: Quy trình khởi động, đóng hệ thống; quy trình sao lưu, phục hồi dữ liệu; quy trình vận hành ứng dụng; quy trình xử lý sự cố; quy trình giám sát và ghi nhật ký hoạt động của hệ thống.

Kiểm soát sự thay đổi của phiên bản phần mềm, cấu hình phần cứng, quy trình vận hành: ghi chép lại các thay đổi; lập kế hoạch, thực hiện kiểm tra, thử nghiệm sự thay đổi, báo cáo kết quả và phải được phê duyệt trước khi áp dụng chính thức.

Hệ thống thông tin vận hành chính thức phải đáp ứng yêu cầu:

- Tách biệt với môi trường phát triển và môi trường kiểm tra, thử nghiệm;

- Áp dụng các giải pháp an ninh, an toàn;

- Không cài đặt các công cụ, phương tiện phát triển ứng dụng trên hệ thống vận hành chính thức.

**Điều 9. Sao lưu dữ liệu**

1. Lập danh sách các dữ liệu, phần mềm cần được sao lưu, có phân loại theo mức độ quan trọng, thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu.

2. Dữ liệu của các hệ thống thông tin quan trọng phải được sao lưu ra phương tiện lưu trữ ngoài (như băng từ, đĩa cứng, đĩa quang hoặc phương tiện lưu trữ khác) và cất giữ, bảo quản an toàn tách rời với khu vực tiến hành sao lưu. Kiểm tra, phục hồi dữ liệu sao lưu từ phương tiện lưu trữ ngoài tối thiểu sáu tháng một lần.

3. Cần tách biệt giữa sao lưu dữ liệu và sao lưu ứng dụng. Mọi ứng dụng được cài đặt hoặc xóa bỏ khỏi hệ thống thông tin đều cần được sao lưu vào hệ thống dự phòng, tách biệt khỏi hệ thống sao lưu dữ liệu.

4. Định kỳ sao lưu hàng tuần, tháng, quý.

**Điều 10. Đảm bảo an toàn, bảo mật trong trao đổi thông tin**

Đơn vị có trách nhiệm:

1. Ban hành quy định về trao đổi thông tin tối thiểu gồm: Phân loại thông tin theo mức độ nhạy cảm; quyền và trách nhiệm của cá nhân khi tiếp cận thông tin; biện pháp đảm bảo tính toàn vẹn, bảo mật khi truyền nhận, xử lý, lưu trữ thông tin; chế độ bảo quản thông tin.

2. Các thông tin, tài liệu, dữ liệu nhạy cảm phải được mã hóa trước khi trao đổi, truyền nhận qua mạng máy tính.

3. Thực hiện các biện pháp quản lý, giám sát và kiểm soát chặt chẽ các trang/cổng thông tin điện tử cung cấp thông tin, dịch vụ, giao dịch trực tuyến cho các tổ chức, cá nhân bên ngoài.

4. Thực hiện biện pháp bảo vệ trang thiết bị, phần mềm phục vụ trao đổi thông tin nội bộ nhằm hạn chế việc xâm nhập, khai thác bất hợp pháp các thông tin nhạy cảm.

**Điều 11. Phòng chống mã độc.**

1. Xác định trách nhiệm của người sử dụng và các bộ phận liên quan trong công tác phòng chống mã độc.

2. Triển khai biện pháp, giải pháp phòng chống mã độc cho toàn bộ hệ thống thông tin của đơn vị.

3. Cập nhập thông tin về các loại mã độc hại mới, triển khai các hành động phòng ngừa tại đơn vị khi có các nguy cơ về các loại mã độc này.

4. Kiểm tra, diệt mã độc đối với vật mang tin nhận từ bên ngoài trước khi sử dụng.

5. Kiểm soát việc cài đặt phần mềm đảm bảo tuân thủ theo quy chế an toàn, an ninh của đơn vị.

6. Xây dựng các kế hoạch phục hồi đối với từng hệ thống CNTT trong trường hợp xảy ra các sự cố về mã độc máy tính.

7. Phối hợp với các cơ quan, đơn vị thường xuyên cập nhật thông tin về các loại mã độc hại mới để có các phương án phòng ngừa các nguy cơ về các loại mã độc này gây ra.

8. Định kỳ hành thánh thống kê, thông báo các sự cố liên quan đến mã độc máy tính trong cơ quan, đơn vị.

**Điều 12. Vai trò, trách nhiệm của cán bộ công chức, viên chức, nhân viên Hàng không.**

a. Vai trò: Nghiêm túc chấp hành các chính sách, quy trình, quy định, hưỡng dẫn, các giải pháp kỹ thuật để đảm bảo an toàn, an ninh thông tin trong các hoạt động nghiệp vụ trong lĩnh vực Hàng không dân dụng.

b. Trách nhiệm: Nắm, hiểu và tuân thủ các quy trình, quy định, chính sách, hướng dẫn về ATTT trong quá trình thực hiện nhiệm vụ được giao hàng ngày, hàng tuần...;

Tham gia quá trình phản ứng sự cố ATTT theo sự điều phối của bộ phận ATTT đơn vị hoặc phối hợp chặt chẽ với các cơ quan, đơn vị trong việc đảm bảo ATTT trên cơ sở các quy định của pháp luật;

Tham gia vào việc triển khai các giải pháp, kế hoạch nhằm đảm bảo ATTT tại cơ quan, đơn vị;

Chịu trách nhiệm nếu vi phạm các chính sách, quy trình, quy định, hưỡng dẫn về ATTT;

Trong quá trình làm nhiệm vụ nếu phát hiện mất ATTT yêu cầu cán bộ công chức, viên chức, nhân viên phải báo cáo ngay với bộ phận ATTT tại cơ quan, đơn vị để kịp thời ngăn chăn, xử lý.

c. Quy định bảo vệ thông tin/dữ liệu: Nghiệm cấm cán bộ công chức, viên chức, nhân viên trong ngành Hàng không thu thập, cung cấp, trao đổi, làm lộ, làm mất, chiếm đoạt, mua bán, tiêu hủy trái phép các thông tin về chủ trương, chính sách của Đảng và nhà nước, các thông tin khác đối với ngành Hàng không.

d. Quy định sử dụng mật khẩu: Phải đặt mật khẩu truy cập máy tính, thiết bị và các phần mềm nội bộ (mail. phần mềm quản lý văn bản...) theo đúng quy định mật khẩu mạnh:

- Có ít nhất 8 ký tự;

- Mật khẩu bao gồm: chữ, số, ký tự đặc biệt;

- Định kỳ đổi mật khẩu theo quy định, đối với mật khẩu máy tính người dùng là 90 ngày;

- Giữ bí mật, không chia sẻ mật khẩu cho người khác. Khi bị lộ mật khẩu, hoặc nghi ngờ mật khẩu bị lộ phải đổi ngay mật khẩu mới, trong trường hợp không thể tự đổi phải làm thủ tục reset mật khẩu theo quy trình quản lý cấp phát tài khảo tương ứng. Khi được cung cấp mật khẩu mới hoặc được reset mật khẩu cần phải đổi ngay mật khẩu mới.

e. Tham gia các chương trình đào tạo, hội nghị về an toàn, an ninh thông tin do Bộ GTVT, Bộ Thông tin và Truyền thông, các cơ quan, đơn vị hoặc các tổ chức có liên quan.

f. Không dùng hòm thư công vụ của cá nhân và của cơ quan, đơn vị vào mục đích cá nhân như đăng ký tài khoản mạng xã hội, đăng ký mua sắm qua mạng...

g. Nghiêm cấm các hành vi sau:

Lợi dụng mạng máy tính, Internet để hoạt động xâm phạm an ninh quốc gia, trật tự an toàn xã hội, vi phạm thuần phong mỹ tục, bản sắc văn hoá Việt Nam, xâm phạm các quyền và lợi ích hợp pháp của tổ chức, công dân cũng như tiến hành các hoạt động tội phạm dưới bất cứ hình thức, phương tiện nào;

Lưu giữ trên máy tính kết nối Internet tin, tài liệu, số liệu thuộc bí mật nhà nước;

Sử dụng mật mã trái với quy định của pháp luật về cơ yếu.

**Chương IV**

**TIẾP NHẬN, PHÁT TRIỂN, DUY TRÌ HỆ THỐNG THÔNG TIN**

**Điều 13. Yêu cầu về an toàn, an ninh cho hệ thống thông tin**

Khi xây dựng mới hoặc cải tiến hệ thống thông tin, đơn vị phải:

1. Xây dựng các yêu cầu về an toàn, an ninh đồng thời với việc đưa ra các yêu cầu kỹ thuật, nghiệp vụ.

2. Đánh giá, xác định cấp độ và tuân thủ đầy đủ các quy định về bảo đảm an toàn thông tin của hệ thống theo cấp độ tương ứng.

3. Xây dựng các yêu cầu về trách nhiệm cập nhật, vá lỗi, khắc phục lỗ hổng bảo mật… (hạn chế để lửng, nên liệt kê đầy đủ) của hệ thống thông tin, được phát hiện trong quá trình vận hành.

4. Xây dựng kế hoạch định kỳ, kiểm tra, rà soát về an toàn an ninh thông tin trong quá trình vận hành hệ thống.

**Điều 14. Đảm bảo an toàn, an ninh các ứng dụng**

Các chương trình ứng dụng nghiệp vụ phải đạt các yêu cầu tối thiểu sau:

1. Kiểm tra tính hợp lệ của dữ liệu đầu vào khi nhập liệu từ người dùng hoặc các hệ thống bên ngoài.

2. Kiểm tra tính hợp lệ của dữ liệu trao đổi giữa các thành phần của hệ thống.

3. Có các biện pháp đảm bảo tính xác thực và tính toàn vẹn dữ liệu.

4. Kiểm tra tính hợp lệ của dữ liệu xuất ra từ các ứng dụng.

5. Mã khóa bí mật của người sử dụng trong các hệ thống thông tin quan trọng phải được mã hóa ở lớp ứng dụng.

**Điều 15. Quản lý mật mã**

1. Quy định và đưa vào sử dụng các biện pháp mã hóa mật mã theo các chuẩn quốc gia hoặc quốc tế đã được công nhận, có biện pháp quản lý khóa để bảo vệ thông tin.

2. Dữ liệu về mã khóa bí mật người sử dụng và các dữ liệu nhạy cảm khác phải được mã hóa, bảo vệ khi truyền qua mạng và khi lưu trữ.

**Điều 16. Quản lý sự thay đổi hệ thống thông tin**

Ban hành quy trình, biện pháp quản lý và kiểm soát sự thay đổi hệ thống thông tin, tối thiểu bao gồm:

1. Có quy định để đảm bảo hệ thống hoạt động ổn định, an toàn khi thay đổi các phần mềm hệ thống như hệ điều hành, hệ quản trị cơ sở dữ liệu;

2. Kiểm soát chặt chẽ việc sửa đổi mã nguồn phần mềm;

3. Giám sát, quản lý chặt chẽ việc thuê mua phần mềm bên ngoài.

**Chương V**

**QUẢN LÝ SẢN PHẨM, DỊCH VỤ CỦA BÊN THỨ BA**

**Điều 17. Ký kết hợp đồng với bên thứ ba**

Đơn vị phải thực hiện:

1. Xác định rõ trách nhiệm, quyền hạn và nghĩa vụ của các bên về an toàn, an ninh công nghệ thông tin khi ký hợp đồng. Hợp đồng với bên thứ ba phải bao gồm các điều khoản và nghĩa vụ về ATTT, cam kết không tiết lộ thông tin, trách nhiệm xử lý, vá lỗ hổng phần mềm, điều khoản xử lý vi phạm và trách nhiệm bồi thường thiệt hại của bên thứ ba do vi phạm của bên thứ ba gây ra.

2. Đơn vị không được thuê bên thứ ba thực hiện toàn bộ công việc quản trị (chỉnh sửa cấu hình, dữ liệu, nhật ký) đối với các hệ thống thông tin quan trọng.

**Điều 18. Trách nhiệm của đơn vị trong quản lý các dịch vụ do bên thứ ba cung cấp**

1. Cung cấp, thông báo và yêu cầu bên thứ ba thực hiện các quy định của đơn vị về an toàn bảo mật hệ thống thông tin.

2. Đơn vị đầu mối làm việc với đối tác phải lập hồ sơ nhật ký giám sát dịch vụ của đối tác cung cấp, bao gồm tốt thiểu các thông tin sau:

- Tên đối tác;

- Dịch vụ cung cấp;

- Ngày thực hiện;

- Các vấn đề về ATTT (sự cố gây giám đoạn, mất hay lộ thông tin, lỗ hổng phần mềm, thời gian khắc phục lỗ hổng…);

- Các thay đổi khác trong dịch vụ (nếu có).

3. Đảm bảo triển khai, duy trì các biện pháp an toàn, an ninh của dịch vụ do bên thứ ba cung cấp theo đúng thỏa thuận.

4. Xác định và ghi rõ các tính năng an toàn, các mức độ bảo mật của dịch vụ và yêu cầu quản lý trong các thỏa thuận về dịch vụ do bên thứ ba cung cấp.

5. Áp dụng các biện pháp giám sát chặt chẽ và giới hạn quyền truy cập của bên thứ ba khi cho phép họ truy cập vào hệ thống thông tin của đơn vị.

6. Giám sát nhân sự của bên thứ ba trong quá trình thực hiện hợp đồng. Khi phát hiện nhân sự bên thứ ba vi phạm quy định về an toàn bảo mật phải thông báo và phối hợp với bên thứ ba áp dụng biện pháp xử lý kịp thời.

7. Thu hồi quyền truy cập hệ thống thông tin đã được cấp cho bên thứ ba, thay đổi các khóa, mã khóa bí mật nhận bàn giao từ bên thứ ba ngay sau khi hoàn thành công việc hoặc kết thúc hợp đồng.

**Điều 19. Trách nhiệm của bên thứ ba khi cung cấp dịch vụ công nghệ thông tin**

1. Ký và thực hiện cam kết bảo mật thông tin cả trong quá trình triển khai và sau khi hoàn tất hợp đồng.

2. Lập kế hoạch, bố trí nhân sự và các nguồn lực khác để thực hiện hợp đồng. Thông báo danh sách nhân sự triển khai cho bên ký kết hợp đồng và phải được đơn vị chấp thuận. Nhân sự bên thứ ba phải ký cam kết không tiết lộ thông tin quan trọng của bên ký kết hợp đồng.

3. Bàn giao tài sản, quyền truy cập hệ thống thông tin do bên ký kết hợp đồng cung cấp khi hoàn thành công việc hoặc kết thúc hợp đồng.

**Chương VI**

**QUẢN LÝ SỰ CỐ AN TOÀN THÔNG TIN MẠNG**

**Điều 20. Quy trình xử lý sự cố**

1. Tiếp nhận thông tin sự cố.

2. Xác thực sự cố.

3. Thông tin cho Lãnh đạo về sự cố.

4. Cô lập hệ thống (bật hệ thống dự phòng nếu có).

5. Thu thập thông tin về sự cố.

6. Phân tích thông tin về sự cố.

7. Xử lý sự cố (yêu cầu hỗ trợ nếu cần).

8. Phục hồi hệ thống (tắt hệ thống dự phòng).

9. Tổng kết đánh giá kết quả.

10. Báo cáo Lãnh đạo và các đơn vị liên quan.

**Điều 21. Nguyên tắc kiểm soát và khắc phục sự cố**

1. Các sự cố mất an toàn thông tin mạng phải được lập tức báo cáo đến những người có thẩm quyền và những người có liên quan.

2. Xác định nguyên nhân và thực hiện các biện pháp phòng ngừa.

3. Quá trình xử lý sự cố phải được ghi chép và lưu trữ. Thực hiện biện pháp bảo vệ, chống chỉnh sửa, hủy hoại đối với tài liệu lưu trữ về sự cố.

4. Thu thập, ghi chép, bảo toàn bằng chứng, chứng cứ phục vụ cho việc kiểm tra, xử lý, khắc phục và phòng ngừa sự cố.

**Chương VII**

**ĐẢM BẢO HOẠT ĐỘNG LIÊN TỤC CỦA**

**CÁC HỆ THỐNG THÔNG TIN**

**Điều 22. Xây dựng hệ thống dự phòng**

1. Đơn vị phải xây dựng hệ thống dự phòng cho các hệ thống thông tin quan trọng.

2. Từng hệ thống dự phòng phải đảm bảo khả năng thay thế hệ thống chính trong thời gian tối đa bốn giờ đồng hồ tính từ thời điểm hệ thống chính có sự cố không khắc phục được.

**Điều 23. Xây dựng quy trình đảm bảo hoạt động liên tục**

1. Xây dựng quy trình xử lý các tình huống gián đoạn hoạt động của từng hệ thống trong hệ thống thông tin như máy chủ, thiết bị mạng,...

2. Quy trình xử lý phải được kiểm tra và cập nhật khi có sự thay đổi của hệ thống thông tin, cơ cấu tổ chức, nhân sự và phân công trách nhiệm của các bộ phận có liên quan trong đơn vị.

3. Hệ thống dự phòng cần được định kỳ kiểm tra để luôn đảm bảo tính sẵn sàng khi xảy ra các sự cố mất an toàn thông tin.

**Chương VIII**

**CHẾ ĐỘ BÁO CÁO**

**Điều 24. Chế độ báo cáo**

Tất cả các cơ quan, đơn vị trong ngành Hàng không dân dụng có trách nhiệm gửi báo cáo về Cục Hàng không Việt Nam (qua Phòng Khoa học, công nghệ và môi trường) như sau:

1. Báo cáo quý, năm

a) Nội dung báo cáo:

- Việc thực hiện bảo đảm an toàn, an ninh thông tin theo quy định tại Quy chế này;

- Kết quả thực hiện nhiệm vụ an toàn thông tin, thống kê các sự cố ATTT, thống kê các hệ thống, ứng dụng mới được triển khai, ý kiến đánh giá, kế hoạch thực hiện tiếp theo và các đề xuất, kiến nghị;

- Các nội dung chỉnh sửa, bổ sung quy chế an toàn, an ninh thông tin của đơn vị (nếu có).

b) Thời hạn gửi báo cáo:

- Báo cáo quý: Gửi trước ngày 25 của tháng cuối quý;

- Báo cáo năm: Gửi trước ngày 25 tháng 12 hàng năm.

2. Báo cáo đột xuất

a) Các sự cố mất an toàn thông tin mạng:

- Thời hạn gửi báo cáo: trong thời gian 03 (ba) ngày kể từ thời điểm vụ, việc được phát hiện;

- Nội dung vụ, việc;

- Thời gian, địa điểm phát sinh vụ, việc;

- Nguyên nhân xảy ra vụ, việc (nếu có);

- Đánh giá rủi ro, ảnh hưởng đối với hệ thống thông tin và nghiệp vụ tại nơi xảy ra vụ, việc và những địa điểm khác có liên quan;

- Các biện pháp đơn vị đã tiến hành để ngăn chặn, khắc phục và phòng ngừa rủi ro.

b. Các cơ quan, đơn vị thực hiện báo cáo đột xuất theo yêu cầu của cơ quan, đơn vị cấp trên.

**Chương IX**

**KHEN THƯỞNG KỶ LUẬT**

**Điều 25. Khen thưởng**

Định kỳ (hàng năm) các cơ quan, đơn vị xem xét, đề xuất khen thưởng, hình thức khen thưởng cho các cá nhân/tập thể có thành tích trong công tác đảm bảo an toàn thông tin.

**Điều 26. Kỷ luật**

Đối với 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 theo trách nhiệm. Nếu gây thiệt hại thì phải bồi thường theo quy định hiện hành của pháp luật.

**Chương III:**

**ĐIỀU KHOẢN THI HÀNH**

**Điều 27. Hiệu lực thi hành**

1. Quy chế này có hiệu lực kể từ ngày ký ban hành.

2. Trong quá trình thực hiện nếu có vấn đề phát sinh, vướng mắc, các đơn vị phản ánh kịp thời về Cục Hàng không Việt Nam (qua Phòng khoa học, công nghệ và môi trường) để xem xét, bổ sung, sửa đổi.

**Điều 28. Trách nhiệm thi hành**

1. Phòng khoa học, công nghệ và môi trường có trách nhiệm:

a) Theo dõi, tổng hợp báo cáo Cục trưởng tình hình thực hiện công tác bảo đảm an toàn, an ninh thông tin của các cơ quan, đơn vị theo quy định tại Quy chế này.

b) Hàng năm lập kế hoạch và kiểm tra việc thực hiện Quy chế này tại các cơ quan, đơn vị.

c) Chủ trì, phối hợp với các đơn vị liên quan trong ngành Hàng không xử lý các vướng mắc phát sinh trong quá trình triển khai thực hiện Quy chế này.

2. Thủ trưởng các cơ quan, đơn vị liên quan trong ngành Hàng không có trách nhiệm tổ chức thực hiện Quy chế này./.

|  |  |
| --- | --- |
|  | **CỤC TRƯỞNG** |
|  |  |