BỘ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 481 /BTTTT-CATTT

Hà Nội, ngày 12 tháng 02 năm 2018

V/v đánh giá mức độ bảo đảm an toàn thông tin mạng

Kính gửi:

- Các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- UBND các tỉnh, thành phố trực thuộc Trung ương.

Căn cứ Quyết định số 898/QĐ-TTg ngày 27/5/2016 của Thủ tướng Chính phủ về phương hướng, mục tiêu, nhiệm vụ bảo đảm an toàn thông tin mạng giai đoạn 2016 - 2020;

Căn cứ Thông báo số 17/TB-VPCP ngày 12/01/2018 của Văn phòng Chính phủ về Kết luận của Phó Thủ tướng Chính phủ Vũ Đức Đam tại phiên họp toàn thể Ủy ban Quốc gia về ứng dụng công nghệ thông tin,

Thực hiện công tác quản lý nhà nước về an toàn thông tin, Bộ Thông tin và Truyền thông chỉ đạo Cục An toàn thông tin phối hợp với Hiệp hội An toàn thông tin Việt Nam (VNISA) tổ chức đánh giá mức độ bảo đảm an toàn thông tin mạng của các bộ, ngành, địa phương. Đây là hoạt động hết sức quan trọng, sẽ được thực hiện hàng năm nhằm đánh giá tổng quát về nhận thức và tình hình triển khai các biện pháp bảo đảm an toàn thông tin mạng tại các bộ, ngành, địa phương.

Bộ Thông tin và Truyền thông gửi mẫu Báo cáo hoạt động bảo đảm an toàn thông tin mạng và trân trọng đề nghị Quý Cơ quan tổng hợp, cung cấp thông tin, số liệu để Bộ Thông tin và Truyền thông đánh giá, báo cáo Thủ tướng Chính phủ.

Quý Cơ quan có thể tải bản mềm mẫu Báo cáo và hướng dẫn chi tiết phương thức thực hiện Cổng Thông tin điện tử của Cục An toàn thông tin tại địa chỉ https://ais.gov.vn.

Báo cáo đề nghị gửi về Bộ Thông tin và Truyền thông theo địa chỉ: Cục An toàn thông tin - Bộ Thông tin và Truyền thông, số 115 Trần Duy Hưng, phường Yên Hòa, quận Cầu Giấy, Hà Nội trước ngày 10 / 3 /2018 cùng với bản mềm về địa chỉ thư điện tử tdkhoa@mic.gov.vn.

Thông tin chi tiết xin liên hệ: Đ/c Trần Đăng Khoa, Phó Trưởng phòng phụ trách, Cục An toàn thông tin, Bộ Thông tin và Truyền thông, thư điện tử:

tdkhoa@mic.gov.vn, điện thoại: 090480480

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Thành Hưng;
- Lưu: VT, CATTT.(130)

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Nguyễn Thành Hưng

Tài liệu gửi kèm theo:
- Mẫu Báo cáo hoạt động bảo đảm an toàn thông tin mạng (Mẫu số 01 và Mẫu số 02);
- Hướng dẫn thực hiện báo cáo hoạt động bảo đảm an toàn thông tin mạng;
- Mẫu tổng hợp danh mục báo cáo (Mẫu số 03);

Mẫu số 01

MẪU BÁO CÁO HOẠT ĐỘNG BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG NĂM 2017

tại các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ,
Ủy ban nhân dân tỉnh, thành phố trực thuộc Trung ương

Stt Câu hỏi

1. Tên cơ quan báo cáo:

.....

2. Đề nghị thống kê số lượng các hệ thống thông tin do cơ quan quản lý trực tiếp vào bảng sau:

Phân loại số lượng HTTT do đơn vị quản lý trực tiếp	Chưa phân loại	Cấp độ 1	Cấp độ 2	Cấp độ 3	Cấp độ 4	Cấp độ 5
Số **HTTT nội bộ đơn vị** (chỉ người trong đơn vị sử dụng)						
Số **HTTT nội bộ dùng chung** (cho nhiều đơn vị trực thuộc cơ quan chủ quản)						
Số **HTTT công cộng** (cung cấp dịch vụ cho cộng đồng vượt quá phạm vi nội bộ như trên)						

3. Có bao nhiêu đơn vị (trực thuộc trực tiếp cơ quan) sử dụng các HTTT nội bộ dùng chung do cơ quan trực tiếp quản lý?

4. Quý cơ quan cung cấp bao nhiêu dịch vụ độc lập (trọn gói) sử dụng cho các đối tượng ngoài cơ quan trong cả nước hoặc phục vụ cộng đồng trên mạng Internet?

5. Cơ quan đã ban hành các chính sách ATTTM (thông tư, quy chế, quy định...) áp dụng cho các hệ thống thông tin của mình chưa? Nếu là có thì ghi số hiệu và năm ban hành các văn bản vào bảng sau và trả lời thêm câu hỏi 6 bên dưới:

Loại văn bản chính sách ATTTM	**Văn bản hiện hành**		**Văn bản cũ trước đây đã được thay thế bằng văn bản hiện hành (nếu có)**	
	Năm	**Số hiệu văn bản**	**Năm**	**Số hiệu văn bản**
Thông tư				
Quy chế, qui định				
Chỉ thị				
Khác				

6. Đề nghị tự nhận xét về chất lượng văn bản hiện hành so với quy định của pháp luật Việt Nam và nhu cầu của cơ quan đến thời điểm hiện tại (chỉ chọn 1 đáp án)?

+ Đầy đủ, chặt chẽ, có thể sử dụng ổn trong khoảng 2 năm trở lên	
+ Tương đối đầy đủ, có thể cần hoàn thiện nhưng sử dụng ổn trong ít nhất 1 năm tới	
+ Đã thấy có các điểm thiếu hoặc không phù hợp, cần sửa đổi hay bổ sung ngay	

7. Trong các quy định, quy chế hiện hành về bảo đảm ATTTM của cơ quan có các nội dung sau đây không?

Quản lý thiết kế an toàn hệ thống thông tin	
Quản lý phát triển phần mềm thuê khoán	
Quản lý thử nghiệm và nghiệm thu hệ thống	
Quản lý vận hành an toàn mạng	
Quản lý vận hành an toàn máy chủ và ứng dụng	
Quản lý an toàn dữ liệu	
Quản lý vận hành an toàn thiết bị đầu cuối	
Quản lý phòng chống phần mềm độc hại	
Quản lý điểm yếu an toàn thông tin	
Quản lý giám sát an toàn hệ thống thông tin	
Quản lý sự cố an toàn thông tin	
Quản lý an toàn người sử dụng đầu cuối	
Quy trình đánh giá, quản lý và xử lý rủi ro về ATTT	
Quy trình thao tác chuẩn để phản ứng khẩn cấp với các sự cố mất ATTTM	

8. Đề nghị tự đánh giá thực tế hiện nay tại cơ quan về mức độ áp dụng thực hiện tốt các quy chế, quy định bảo đảm ATTTM đạt khoảng độ bao nhiêu phần trăm theo thang điểm 100%

9. Tổng số cán bộ, công chức, viên chức, người lao động đang làm việc trong cơ quan

10. Tổng số cán bộ lãnh đạo quản lý (cấp cơ quan và cấp vụ/tương đương trực thuộc cơ quan) của cơ quan

11. Số người sử dụng máy tính hiện tại trong cơ quan

12. Cơ quan có phân công lãnh đạo (cấp cơ quan) phụ trách về ATTTM hay không?

13. Cơ quan có tổ chức/bộ phận chuyên trách về ATTTM hay không? (Nếu có trả lời thêm câu 16 dưới đây)

14. Vị trí và quan hệ công tác của bộ phận chuyên trách về ATTTM (có thể lựa chọn nhiều đáp án)

Là bộ phận con thuộc tổ chức phụ trách CNTT của đơn vị	
Chịu sự chỉ đạo nghiệp vụ của bộ phận chuyên trách ATTTM của cơ quan chủ quản	
Là thành viên thuộc mạng lưới chuyên trách bảo đảm ATTT của quốc gia	
Có quy chế phối hợp xử lý sự cố ATTTM với doanh nghiệp cung cấp dịch vụ mạng	
Có quy chế phối hợp xử lý sự cố ATTTM với các tổ chức ATTTM khác. Ví dụ:	

15. Tổng số cán bộ làm việc chuyên trách về ATTTM

16. Tổng số cán bộ làm việc bán chuyên trách về ATTTM

17. Quản lý nhân sự phù hợp yêu cầu ATTT như thế nào? - Có quy định từng khâu? Thực hiện đầy đủ không? (mỗi cột lựa chọn 1 đáp án)

Quản lý nhân sự về ATTT trong từng khâu	**Tuyển dụng cán bộ ATTT**	**Quản lý quá trình làm việc**	**Chấm dứt, chuyển công việc**
Chưa có quy định cụ thể			
Có quy định, thực hiện chưa tốt thường xuyên			
Có quy định, thực hiện tốt			

18. Tổng số cán bộ nhân viên đã từng được qua lớp đào tạo, tập huấn về ATTTM

19. Tổng số cán bộ lãnh đạo quản lý (cấp cơ quan và cấp vụ/tương đương trực thuộc cơ quan) đã từng được đào tạo, tập huấn về quản lý ATTTM

20. Tổng số cán bộ kỹ thuật có trình độ tương đương đại học ngành ATTT trở lên

21. Tổng số cán bộ kỹ thuật có trình độ tương đương trung cấp về ATTT

22. Tổng số chuyên gia chuyên sâu về ATTTM

23. Cơ quan có kế hoạch đào tạo, tập huấn chung cho các đơn vị trực thuộc về ATTTM trong năm 2017 không?

24. Hãy cho biết kết quả đào tạo, tập huấn năm 2017 về ATTTM của cơ quan theo bảng sau:

Số người được đào tạo, tập huấn	**Theo kế hoạch chung của cấp trên tổ chức**	**Theo kế hoạch riêng của đơn vị**
Số cán bộ lãnh đạo		
Số cán bộ, nhân viên chuyên trách ATTTM		
Số cán bộ, nhân viên khác sử dụng máy tính		

25. Cơ quan có kế hoạch định kỳ tuyên truyền, phổ biến nâng cao nhận thức của người sử dụng về ATTTM năm 2017 hay không?

26. Số đơn vị trực thuộc các cơ quan khác được thụ hưởng kế hoạch tuyên truyền, phổ biến nâng cao nhận thức về ATTTM mà đơn vị triển khai trong năm 2017

27. Cơ quan có chủ trương hay quy định thuê ngoài (out-source) các dịch vụ về bảo đảm ATTTM không?

+ Không có chủ trương hay quy định thuê ngoài	
+ Có chủ trương nhưng chưa có thuê ngoài	
+ Đã thuê ngoài dịch vụ bảo đảm ATTTM	

28. Cơ quan có chủ trương sử dụng dịch vụ thuê hosting hệ thống (thuê ngoài hệ thống máy chủ và lưu trữ cơ sở dữ liệu) do các công ty Việt Nam không có yếu tố nước ngoài cung cấp hay không?

+ Không có chủ trương này	
+ Có chủ trương nhưng chưa có thuê	
+ Đã thuê dịch vụ của các công ty Việt Nam không có yếu tố nước ngoài	

29. Cơ quan có chủ trương sử dụng dịch vụ thuê hosting hệ thống có yếu tố nước ngoài cung cấp hay sử dụng dịch vụ điện toán đám mây (cloud computing) trên Internet hay không?

+ Không có chủ trương này	
+ Có chủ trương nhưng chưa sử dụng dịch vụ này	
+ Đã sử dụng dịch vụ này	

30. Cơ quan bảo đảm ATTTM thường xuyên bằng cách nào:

+ Hoàn toàn sử dụng nội lực	
+ Sử dụng toàn bộ thuê và hỗ trợ từ bên ngoài	
+ Sử dụng một phần nội lực, một phần lực lượng bên ngoài	

31. Cơ quan có tổng chi (bao gồm cả chi ngân sách thường xuyên và dự án đầu tư) cho CNTT trong 3 năm gần đây là bao nhiêu (xTriệu đồng)?

Chi cho CNTT	2015	2016	2017
Tổng chi (xTriệu đồng)			

32. Ước tính tỷ lệ chi cho ATTTM chiếm bao nhiêu % trong tổng đầu tư dành cho CNTT tại cơ quan trong 3 năm gần đây?

Chi cho ATTTM so với chi CNTT	2015	2016	2017
Tỷ lệ chi ATTTM/chi CNTT (%)			

33. Ước tính tỷ lệ chi cho ATTTM cho các hệ thống thông tin quan trọng quốc gia do cơ quan quản lý chiếm bao nhiêu % trong tổng đầu tư CNTT của đơn vị trong 3 năm gần

đây?

Chi ATTTM so với chi CNTT cho HTTT quan trọng quốc gia	2015	2016	2017
Tỷ lệ chi ATTTM/chi CNTT (%)			

34. Ước tính chi phí chung về ATTTM năm 2017 đáp ứng bao nhiêu % nhu cầu (dự toán) của cơ quan?

Mức đáp ứng nhu cầu chi hàng năm về ATTTM	2015	2016	2017
Tỷ lệ chi ATTTM/nhu cầu (%)			

35. Cơ quan đã triển khai hệ thống quản lý ATTTM (hệ thống ISMS) theo tiêu chuẩn TCVN/ISO-IEC 27000 hoặc tiêu chuẩn TCVN 11930: 2017 hay tiêu chuẩn khác chưa?
(Ghi rõ tiêu chuẩn khác là: .....)

36. Cơ quan đã nhận chứng nhận hợp chuẩn quản lý ATTTM theo 1 trong những tiêu chuẩn trên chưa? Nếu có thì cho biết thời điểm chứng nhận đã cách thời điểm hiện tại bao nhiêu tháng theo bảng dưới đây:

Thời điểm hợp chuẩn	Lần đầu tiên	Lần gần đây nhất
Cách đây bao nhiêu tháng		

37. Cơ quan có bao nhiêu hệ thống thông tin quan trọng quốc gia (cấp độ 5) hoặc hệ thống thông tin cấp độ 4 thuộc trách nhiệm quản lý đã nhận chứng nhận hợp chuẩn quản lý ATTTM ?

HTTT đã được hợp chuẩn	Hệ thống cấp độ 5	Hệ thống cấp độ 4	Hệ thống quan trọng quốc gia khác
Số lượng HTTT đã hợp chuẩn			

38. Cơ quan có thực hiện các biện pháp phân loại, xác định trách nhiệm về sở hữu tài sản thông tin hay không ?

39. Việc quản lý cán bộ vận hành, khai thác, sử dụng hệ thống của cơ quan có tuân thủ các chính sách về ATTTM hay không?

40. Cơ quan có quy trình đánh giá, quản lý và xử lý rủi ro về ATTTM không?

41. Cơ quan có quy trình thao tác chuẩn (Standard operating procedures) để phản ứng với các sự cố mất ATTT hay không?

42. Trong quá trình triển khai dự án phát triển ứng dụng CNTT, cơ quan có thực hiện tư vấn, thẩm định, thẩm tra về ATTTM của hệ thống thông tin được xây dựng hay không?

43. Tổng số lần cơ quan đã thực hiện kiểm tra đánh giá ATTTM định kỳ cho hệ thống thông tin của mình trong năm 2017 ?

44. Tổng số lần cơ quan đã tổ chức hoặc trực tiếp tham gia diễn tập bảo đảm ATTTM cho hệ thống thông tin của mình trong năm 2017 ?

45. Với các biện pháp kỹ thuật, công nghệ phù hợp đang được cơ quan đang áp dụng để bảo đảm ATTTM cho các HTTT nội bộ và HTTT công cộng, hãy cho biết lần trang bị, cập nhật, nâng cấp hay làm mới **gần đây nhất** là cách thời điểm hiện tại bao nhiêu tháng (tính cả tháng hiện tại) ?

Các biện pháp kỹ thuật, công nghệ bảo đảm an toàn mạng được trang bị, cập nhật, nâng cấp hay làm mới gần đây nhất cách hiện nay bao nhiêu tháng	**HTTT nội bộ**	**HTTT công cộng**
+ Hệ thống thiết bị sensor ghi log-file phát hiện sự cố và mối đe dọa ATTT đối với mạng		
+ Hệ thống giám sát và quản lý sự kiện an toàn thông tin (SOC-Security Operation Center/SIEM- Security Incident & Event Management)		
+ Giải pháp phân chia hệ thống mạng thành các vùng mạng chức năng với các chính sách quản lý và biện pháp kỹ thuật ATTTM phù hợp		
+ Hệ thống phát hiện xâm nhập (IDS/IPS) trong mạng		
+ Hệ thống phòng chống tấn công DoS/DDoS		
+ Tường lửa cho toàn mạng (Network Firewall)		
+ Phần mềm chống virus mức mạng (Anti-Virus)		
+ Bảo vệ kênh truyền bằng công nghệ mã hóa và xác thực		
+ Kiểm soát mọi kênh truy cập có bắt buộc định kỳ thay đổi mật khẩu người dùng		
+ Kiểm soát mọi kênh truy cập có giải pháp hạn chế đăng nhập tự động (tấn công kiểu từ điển) và/hoặc có yêu cầu xác thực hai yếu tố người dùng		
+ Bảo mật truy cập qua mạng không dây và các thiết bị đầu cuối		

46. Với các biện pháp kỹ thuật, công nghệ phù hợp đang được cơ quan áp dụng để bảo vệ các hệ thống máy chủ trong các HTTT nội bộ và HTTT công cộng, hãy cho biết lần trang bị, cập nhật, nâng cấp hay làm mới **gần đây nhất** là cách thời điểm hiên tại bao nhiêu tháng (tính cả tháng hiện tại) ?

Các công nghệ, biện pháp kỹ thuật bảo vệ các hệ thống máy chủ được trang bị, cập nhật, nâng cấp hay làm mới gần đây nhất cách hiện nay bao nhiêu tháng	**HTTT nội bộ**	**HTTT công cộng**
+ Hệ thống quản lý thu thập và phân tích log-file phát hiện sự cố và mối đe dọa ATTT		

+ Hệ thống phát hiện và chống tấn công xâm nhập máy chủ (IDS/IPS)		
+ Tường lửa (Firewall) cho máy chủ		
+ Phần mềm chống virus mã độc (Anti-Virus)		
+ Quản lý phân chia người dùng theo đặc quyền và có theo dõi phát hiện tài khoản người dùng lạ trong hệ thống		
+ Quản lý truy cập và chống tấn công leo thang đặc quyền		
+ Bảo mật thiết bị di động và thiết bị đầu cuối truy cập từ xa		
+ Sử dụng hệ thống máy chủ dự phòng nóng (chạy song song, on-line)		
+ Sử dụng hệ thống máy chủ dự trữ (dự phòng off-line)		

47. Với các biện pháp kỹ thuật, công nghệ phù hợp đang được cơ quan đang áp dụng để bảo vệ các ứng dụng trong các HTTT nội bộ và HTTT công cộng, hãy cho biết lần trang bị, cập nhật, nâng cấp hay làm mới gần đây nhất là cách thời điểm hiên tại bao nhiêu tháng (tính cả tháng hiện tại) ?

Các công nghệ, biện pháp kỹ thuật phù hợp bảo vệ các ứng dụng được trang bị, cập nhật, nâng cấp hay làm mới gần đây nhất cách hiện nay bao nhiêu tháng	**HTTT nội bộ**	**HTTT công cộng**
+ Hệ thống ghi nhật ký (log-file) các ứng dụng		
+ Hệ thống quản lý và phân tích log-file		
+ Quản lý truy cập có xác thực nhiều bước		
+ Phần mềm chống virus mã độc (Anti-Virus)		
+ Tường lửa mức ứng dụng (ví dụ web-firewall,...)		
+ Lọc nội dung Web		
+ Bộ lọc chống thư rác (Anti-Spam)		
+ Sử dụng hệ thống máy chủ dự phòng nóng (chạy song song, on-line)		
+ Sử dụng hệ thống máy chủ dự trữ (dự phòng off-line)		

48. Với các biện pháp kỹ thuật, công nghệ phù hợp đang được cơ quan đang áp dụng để bảo vệ dữ liệu cho các HTTT nội bộ và HTTT công cộng, hãy cho biết lần trang bị, cập nhật, nâng cấp hay làm mới **gần đây nhất** là cách thời điểm hiên tại bao nhiêu tháng (tính cả tháng hiện tại) ?

Các biện pháp kỹ thuật, công nghệ phù hợp bảo vệ dữ liệu được trang bị, cập nhật, nâng cấp hay làm mới gần đây nhất cách hiện nay bao nhiêu tháng	**HTTT nội bộ**	**HTTT công cộng**
+ Hệ thống giám sát tính toàn vẹn CSDL		
+ Hệ thống phát hiện xâm nhập CSDL		

+ Bảo vệ dữ liệu quan trọng trong hệ thống bằng công nghệ mã hóa		
+ Bảo vệ dữ liệu quan trọng trong hệ thống bằng công nghệ chữ ký số		
+ Hệ thống quản lý chống thất thoát dữ liệu (Data Loss protection)		
+ Sử dụng hệ thống sao lưu dữ liệu dự phòng nóng (on-line back-up)		
+ Sử dụng hệ thống sao lưu dữ liệu dự phòng định kỳ (off-line back-up)		

49. Với các biện pháp kỹ thuật, công nghệ phù hợp đang được cơ quan đang áp dụng để bảo đảm an toàn về mặt vật lý cho các HTTT nội bộ và HTTT công cộng, hãy cho biết lần trang bị, cập nhật, nâng cấp hay làm mới **gần đây nhất** là cách thời điểm hiện tại bao nhiêu tháng (tính cả tháng hiện tại) ?

Các biện pháp kỹ thuật, công nghệ phù hợp bảo đảm an toàn vật lý được trang bị, cập nhật, nâng cấp hay làm mới gần đây nhất cách thời điểm hiện tại bao nhiêu tháng	**HTTT nội bộ**	**HTTT công cộng**
+ Giải pháp lựa chọn vị trí vật lý		
+ Giải pháp kiểm soát truy cập vật lý		
+ Giải pháp chống trộm, chống phá hoại		
+ Giải pháp chống sét		
+ Hệ thống chống cháy nổ		
+ Giải pháp chống ẩm và chống thấm		
+ Giải pháp chống bụi và tĩnh điện		
+ Giải pháp kiểm soát nhiệt độ và độ ẩm		
+ Hệ thống nguồn cung cấp điện dự phòng		
+ Giải pháp bảo vệ điện từ trường		

50. Cơ quan có khả năng ghi nhận các hành vi tấn công (kể cả chưa thành công) vào hệ thống của mình hay không? | |

51. Khi hệ thống của cơ quan gặp sự cố mất ATTTM, quý vị sẽ báo cáo/thông báo tin này đi đâu? Đánh dấu tương ứng vào các ô phù hợp trong bảng sau:

Phản ứng / Loại sự cố, nguy cơ ATTTM	Tự xử lý, không báo cáo	Mời DN, sử dụng dịch vụ ngoài	Báo cáo cấp trên, ngành dọc	Báo và hợp tác với nhà mạng	Báo và hợp tác với đơn vị Bộ Quốc phòng	Báo và hợp tác với đơn vị Bộ Công an	Báo và hợp tác với đơn vị Bộ TTTT

Đơn vị đủ khả năng phát hiện và xử lý							
Đơn vị phát hiện được, chưa gây tác hại, nhưng khó xử lý							
Loại mới hoặc tấn công gây tác hại lớn, chưa tự xử lý được							

52. Từ 01/01/2017 đến hết 31/12/2017, cơ quan đã phát hiện được bao nhiêu sự cố ATTTM vào hệ thống của mình chưa gây ra thiệt hại hoặc gây ra thiệt hại nhỏ? Thống kê số vụ tấn công mạng đã xảy ra với các hệ thống thông tin do cơ quan quản lý (phân loại theo kiểu tấn công và hậu quả).

Số vụ tấn công mạng ít nghiêm trọng từ 01/01/2017 đến hết 31/12/2017	Số vụ tấn công web deface hay cài Phishing	Số lần tấn công từ chối dịch vụ (DDoS)	Số vụ tấn công bằng thư điện tử (spam)	Số máy tính trạm đã bị lây nhiễm mã độc	Số lần máy chủ bị tấn công bằng mã độc	Số vụ tấn công vào lỗ hổng ATTT của HTTT	Số sự cố khác (lỗi hạ tầng, vật lý, phần mềm)	Số vụ xâm nhập mạng do ATP, lộ mật khẩu
Số vụ đã phát hiện và ngăn chặn sớm, chưa gây ra thiệt hại								
Số vụ tấn công đã bị xâm nhập, lây nhiễm mã độc, nhưng chỉ gây ra thiệt hại nhỏ								

53. Số vụ tấn công, mất ATTTM nghiêm trọng (gây ra hậu quả nghiêm trọng về kinh tế, gián đoạn dịch vụ mạng, lộ lọt thông tin quan trọng...) xảy ra từ 01/01/2017 đến hết 31/12/2017

Số vụ việc mất ATTTM nghiêm trọng xảy ra từ	Số lần tấn công từ chối dịch vụ (DDoS)	Số lần máy chủ bị	Số máy tính trạm đã bị	Số vụ xâm nhập mạng do	Số vụ tấn công vào lỗ hổng	Số vụ tấn công web deface hay cài	Số vụ tấn công bằng thư	Số sự cố khác (lỗi hạ tầng,

01/01/2017 đến hết 31/12/2017		tấn công bằng mã độc	lây nhiễm mã độc	ATP, lộ mật khẩu	ATTT của HTTT	Phishing	điện tử (spam -mail)	vật lý, phần mềm)
Tổng số vụ việc đã phát hiện, xử lý								
Đơn vị tự xử lý, khắc phục hậu quả thành công trong vòng 24h								
Được đơn vị khác hỗ trợ xử lý, khắc phục hậu quả thành công trong vòng 24h								

54. Theo quý vị những động cơ nào được nghi ngờ là nguyên nhân gây ra những hành động tấn công ở trên? (Có thể chọn nhiều đáp án là các mục sau)

Nhằm thể hiện kỹ năng tấn công	
Phá hoại hệ thống có chủ đích	
Nhằm chiếm dụng tài nguyên hệ thống để dẫn tới những cuộc tấn công nặc danh	
Thù hằn cá nhân (ví dụ: cán bộ hoặc người ngoài có thù hằn cá nhân)	
Nhằm tạo lợi thế cạnh tranh thương mại (ví dụ: tình báo công nghiệp)	
Chiếm đoạt tài nguyên hệ thống của cơ quan để sử dụng cho mục đích cá nhân	
Bị tấn công từ nước ngoài do các nguyên nhân liên quan đến chủ quyền	
Tạo nguồn thu tài chính bất hợp pháp	
Nhằm chiếm dụng tài nguyên hệ thống để dẫn tới những cuộc tấn công nặc danh	
Thù hằn cá nhân (ví dụ: cán bộ hoặc người ngoài có thù hằn cá nhân)	

55. Với tình hình hiện tại thì trong thời gian tới, đối tượng đe dọa tới ATTTM của hệ thống mà quý cơ quan lo ngại nhất là gì ? (Ghi các số 1/2/3 tương ứng với các hạng mục lo ngại nhất, nhì và ba)

- Cán bộ đang làm việc tại công ty	
- Cán bộ đã nghỉ việc tại công ty	
- Tội phạm máy tính như *hacker* bất hợp pháp	
- Đối thủ cạnh tranh (*gián điệp công nghiệp*)	
- Băng nhóm tội phạm máy tính có tổ chức (*khủng bố mạng* v.v...)	
- Doanh nghiệp gia công bên ngoài (nhân viên) Outsourcing company (employees)	
- Các thế lực đến từ nước ngoài	
- Những mối đe dọa khác (vui lòng ghi rõ):	

56. Những vấn đề khó khăn nhất mà cơ quan gặp phải trong việc bảo đảm ATTTM cho hệ thống thông tin là gì? (Ghi các số 1/2/3/4/5 tương ứng với các hạng mục khó khăn nhất, nhì, ba, tư và năm)

Lãnh đạo chưa hỗ trợ đúng mức cần thiết cho ATTTM	
Sự thiếu hiểu biết về ATTTM trong đơn vị, thiếu cán bộ am hiểu kỹ thuật và quản lý ATTTM	
Việc nâng cao nhận thức và mặt bằng kiến thức cho người sử dụng máy tính về ATTTM	
Việc xác định chính xác mức độ ưu tiên của ATTTM trong tương quan chung với các vấn đề khác của đơn vị	
Việc áp dụng các nguyên tắc quản lý rủi ro (Risk Management principles) cho hệ thống thông tin	
Việc cập nhật kịp thời những cách thức tấn công hay những những điểm yếu mới xuất hiện	
Việc giám sát phát hiện, cảnh báo sớm các cuộc tấn công mạng	
Không đủ khả năng phản ứng nhanh và xử lý chính xác khi xảy ra những vụ tấn công qua mạng	
Việc quản lý chặt chẽ cấu hình hệ thống mạng (Configuration Management)	
Những hệ thống máy tính không được quản lý tốt	
Kinh phí/ngân sách dành cho ATTTM quá thiếu so với mặt bằng chung	
Các vấn đề khác (Nếu có thì vui lòng ghi rõ):	

57. Số lần cơ quan đã rút kinh nghiệm bài học khắc phục sự cố dẫn đến việc thay đổi, bổ sung, hoàn thiện quy định, quy chế ứng cứu sự cố và bảo đảm ATTTM trong năm 2017 | |

58. Cơ quan có sử dụng chữ ký số để bảo đảm an toàn cho các giao dịch điện tử hay không? | |

Lãnh đạo đơn vị
(Ký, ghi rõ họ tên và đóng dấu)

Người lập bảng khảo sát

Họ tên:.....

Điện thoại:.....

Email:.....

Báo cáo đã điền đầy đủ nội dung xin gửi về Cục An toàn thông tin, Bộ Thông tin và Truyền thông, địa chỉ: tầng 8, số 115 Trần Duy Hưng, Hà Nội.

Mẫu số 02

MẪU BÁO CÁO HOẠT ĐỘNG BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG NĂM 2017

tại đơn vị trực thuộc trực tiếp các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân tỉnh, thành phố trực thuộc Trung ương

Stt Câu hỏi

1. Tên đơn vị báo cáo:

.....

Cơ quan chủ quản:

.....

2. Đề nghị thống kê số lượng các hệ thống thông tin do đơn vị quản lý trực tiếp vào bảng sau:

Phân loại số lượng HTTT do đơn vị quản lý trực tiếp	Chưa phân loại	Cấp độ 1	Cấp độ 2	Cấp độ 3	Cấp độ 4	Cấp độ 5
Số **HTTT nội bộ đơn vị** (chỉ người trong đơn vị sử dụng)						
Số **HTTT nội bộ dùng chung** (cho nhiều đơn vị trực thuộc cơ quan chủ quản)						
Số **HTTT công cộng** (cung cấp dịch vụ cho cộng đồng vượt quá phạm vi nội bộ như trên)						

3. Có bao nhiêu đơn vị (trực thuộc trực tiếp cơ quan chủ quản) sử dụng các HTTT nội bộ dùng chung do Quý đơn vị trực tiếp quản lý?

4. Quý đơn vị cung cấp bao nhiêu dịch vụ độc lập (trọn gói) sử dụng cho các đối tượng ngoài cơ quan chủ quản trong cả nước hoặc phục vụ cộng đồng trên mạng Internet?

5. Đơn vị có ban hành quy chế, quy định riêng hoặc có áp dụng quy chế, quy định chung của cơ quan chủ quản về bảo đảm ATTTM không? Nếu có thì điền nội dung phù hợp vào bảng sau và trả lời thêm câu 6 và câu 7 dưới đây (nếu không có thì để trống)

Loại văn bản chính sách ATTTM được đơn vị áp dụng	**Văn bản hiện hành**		**Văn bản cũ trước đây đã được thay thế bằng văn bản hiện hành (nếu có)**	
	Năm	**Số hiệu văn bản**	**Năm**	**Số hiệu văn bản**
Quy định riêng				
Quy chế chung				

6. Trong các quy định, quy chế hiện hành về bảo đảm ATTTM của đơn vị có các nội dung sau đây không?

Quản lý thiết kế an toàn hệ thống thông tin		
Quản lý phát triển phần mềm thuê khoán		
Quản lý thử nghiệm và nghiệm thu hệ thống		
Quản lý vận hành an toàn mạng		
Quản lý vận hành an toàn máy chủ và ứng dụng		
Quản lý an toàn dữ liệu		
Quản lý vận hành an toàn thiết bị đầu cuối		
Quản lý phòng chống phần mềm độc hại		
Quản lý điểm yếu an toàn thông tin		
Quản lý giám sát an toàn hệ thống thông tin		
Quản lý sự cố an toàn thông tin		
Quản lý an toàn người sử dụng đầu cuối		
Quy trình đánh giá, quản lý và xử lý rủi ro về ATTT		
Quy trình thao tác chuẩn để phản ứng khẩn cấp với các sự cố mất ATTTM		

7. Đề nghị tự nhận xét về chất lượng của quy định, quy chế hiện hành so với quy định của pháp luật Việt Nam và nhu cầu của đơn vị đến thời điểm hiện tại (chọn 1 đáp án)?

+ Đầy đủ, chặt chẽ, có thể sử dụng ổn trong khoảng 2 năm trở lên	
+ Tương đối đầy đủ, có thể cần hoàn thiện nhưng sử dụng ổn trong ít nhất 1 năm tới	
+ Đã thấy có các điểm thiếu hoặc không phù hợp, cần sửa đổi hay bổ sung ngay	

8. Đề nghị tự đánh giá thực tế hiện nay tại đơn vị về mức độ áp dụng thực hiện tốt các quy chế, quy định bảo đảm ATTTM đạt khoảng độ bao nhiêu phần trăm theo thang điểm 100%

9. Tổng số cán bộ, công chức, viên chức, người lao động đang làm việc trong đơn vị

10. Tổng số cán bộ lãnh đạo quản lý (cấp đơn vị và cấp phòng/tương đương trực thuộc đơn vị) của đơn vị

11. Số người sử dụng máy tính hiện tại trong đơn vị

12. Đơn vị có phân công lãnh đạo (cấp đơn vị) phụ trách về ATTTM hay không?

13. Đơn vị có tổ chức/bộ phận chuyên trách về ATTTM hay không? (Nếu có trả lời thêm câu 16 dưới đây)

14. Vị trí và quan hệ công tác của bộ phận chuyên trách về ATTTM (có thể lựa chọn nhiều đáp án)

Là bộ phận con thuộc tổ chức phụ trách CNTT của đơn vị	
Chịu sự chỉ đạo nghiệp vụ của bộ phận chuyên trách ATTTM của cơ quan chủ quản	
Là thành viên thuộc mạng lưới chuyên trách bảo đảm ATTT của quốc gia	
Có quy chế phối hợp xử lý sự cố ATTTM với doanh nghiệp cung cấp dịch vụ mạng	
Có quy chế phối hợp xử lý sự cố ATTTM với các tổ chức ATTTM khác. Ví dụ:	

15. Tổng số cán bộ làm việc chuyên trách về ATTTM
16. Tổng số cán bộ làm việc bán chuyên trách về ATTTM
17. Quản lý nhân sự phù hợp yêu cầu ATTT như thế nào? - Có quy định từng khâu? Thực hiện đầy đủ không? (mỗi cột lựa chọn 1 đáp án)

Quản lý nhân sự về ATTT trong từng khâu	**Tuyển dụng cán bộ ATTT**	**Quản lý quá trình làm việc**	**Chấm dứt, chuyển công việc**
Chưa có quy định cụ thể			
Có quy định, thực hiện chưa tốt thường xuyên			
Có quy định, thực hiện tốt			

18. Tổng số cán bộ nhân viên đã từng được qua lớp đào tạo, tập huấn về ATTTM
19. Tổng số cán bộ lãnh đạo quản lý (cấp đơn vị và cấp phòng/tương đương trực thuộc đơn vị) đã từng được đào tạo, tập huấn về quản lý ATTTM
20. Tổng số cán bộ kỹ thuật có trình độ tương đương đại học ngành ATTT trở lên
21. Tổng số cán bộ kỹ thuật có trình độ tương đương trung cấp về ATTT
22. Tổng số chuyên gia chuyên sâu về ATTTM
23. Đơn vị có kế hoạch đào tạo, tập huấn riêng về ATTTM trong năm 2017 hay không?
24. Hãy cho biết kết quả đào tạo, tập huấn năm 2017 về ATTTM của quý đơn vị theo bảng sau:

Số người được đào tạo, tập huấn	**Theo kế hoạch chung của cấp trên tổ chức**	**Theo kế hoạch riêng của đơn vị**
Số cán bộ lãnh đạo		
Số cán bộ, nhân viên chuyên trách ATTTM		
Số cán bộ, nhân viên khác sử dụng máy tính		

25. Đơn vị có được thụ hưởng kế hoạch tuyên truyền, phổ biến nâng cao nhận thức về ATTTM của cấp trên (cơ quan chủ quản, cơ quan quản lý nhà nước) trong năm 2017 hay không?

26. Quý đơn vị có thực hiện kế hoạch riêng tuyên truyền, phổ biến nâng cao nhận thức về ATTTM trong năm 2017 hay không?

27. Số đơn vị trực thuộc cùng cơ quan chủ quản được thụ hưởng kế hoạch tuyên truyền, phổ biến nâng cao nhận thức về ATTTM mà quý đơn vị triển khai trong năm 2017

28. Số đơn vị trực thuộc các cơ quan chủ quản khác được thụ hưởng kế hoạch tuyên truyền, phổ biến nâng cao nhận thức về ATTTM mà đơn vị triển khai trong năm 2017

29. Đơn vị có chủ trương sử dụng dịch vụ thuê hosting hệ thống (thuê ngoài hệ thống máy chủ và lưu trữ cơ sở dữ liệu) do các công ty Việt Nam không có yếu tố nước ngoài cung cấp hay không?

+ Không có chủ trương này	
+ Có chủ trương nhưng chưa có thuê	
+ Đã thuê dịch vụ của các công ty Việt Nam không có yếu tố nước ngoài	

30. Đơn vị có chủ trương sử dụng dịch vụ thuê hosting hệ thống có yếu tố nước ngoài cung cấp hay sử dụng dịch vụ điện toán đám mây (cloud computing) trên Internet hay không?

+ Không có chủ trương này	
+ Có chủ trương nhưng chưa sử dụng dịch vụ này	
+ Đã sử dụng dịch vụ này	

31. Đơn vị bảo đảm ATTTM thường xuyên bằng cách nào:

+ Hoàn toàn sử dụng nội lực	
+ Sử dụng toàn bộ thuê và hỗ trợ từ bên ngoài	
+ Sử dụng một phần nội lực, một phần lực lượng bên ngoài	

32. Đơn vị có tổng chi (bao gồm cả chi ngân sách thường xuyên và dự án đầu tư) cho CNTT trong 3 năm gần đây là bao nhiêu (xTriệu đồng)?

Chi cho CNTT	2015	2016	2017
Tổng chi (xTriệu đồng)			

33. Ước tính tỷ lệ chi cho ATTTM chiếm bao nhiêu % trong tổng đầu tư dành cho CNTT tại đơn vị trong 3 năm gần đây?

Chi cho ATTTM so với chi CNTT	2015	2016	2017
Tỷ lệ chi ATTTM/chi CNTT (%)			

34. Ước tính tỷ lệ chi cho ATTTM cho các hệ thống thông tin quan trọng quốc gia do đơn

vị quản lý chiếm bao nhiêu % trong tổng đầu tư CNTT của đơn vị trong 3 năm gần đây?

Chi ATTTM so với chi CNTT cho HTTT quan trọng quốc gia	**2015**	**2016**	**2017**
Tỷ lệ chi ATTTM/chi CNTT (%)			

35. Ước tính chi phí chung về ATTTM năm 2017 đáp ứng bao nhiêu % nhu cầu (dự toán) của đơn vị?

Mức đáp ứng nhu cầu chi hàng năm về ATTTM	**2015**	**2016**	**2017**
Tỷ lệ chi ATTTM/nhu cầu (%)			

36. Đơn vị đã triển khai hệ thống quản lý ATTTM (hệ thống ISMS) theo tiêu chuẩn TCVN/ISO-IEC 27000 hoặc tiêu chuẩn TCVN 11930: 2017 hay tiêu chuẩn khác chưa?
(Ghi rõ tiêu chuẩn khác là: .....)

37. Đơn vị đã nhận chứng nhận hợp chuẩn quản lý ATTTM theo 1 trong những tiêu chuẩn trên chưa? Nếu có thì cho biết thời điểm chứng nhận đã cách thời điểm hiện tại bao nhiêu tháng theo bảng dưới đây:

Thời điểm hợp chuẩn	**Lần đầu tiên**	**Lần gần đây nhất**
Cách đây bao nhiêu tháng		

38. Đơn vị có bao nhiêu hệ thống thông tin quan trọng quốc gia (cấp độ 5) hoặc hệ thống thông tin cấp độ 4 thuộc trách nhiệm quản lý đã nhận chứng nhận hợp chuẩn quản lý ATTTM?

HTTT đã được hợp chuẩn	**Hệ thống cấp độ 5**	**Hệ thống cấp độ 4**	**Hệ thống quan trọng quốc gia khác**
Số lượng HTTT đã hợp chuẩn			

39. Đơn vị có thực hiện các biện pháp phân loại, xác định trách nhiệm về sở hữu tài sản thông tin hay không ?

40. Việc quản lý cán bộ vận hành, khai thác, sử dụng hệ thống của đơn vị có tuân thủ các chính sách về ATTTM hay không?

41. Đơn vị có quy trình đánh giá, quản lý và xử lý rủi ro về ATTTM không?

42. Đơn vị có quy trình thao tác chuẩn (Standard operating procedures) để phản ứng với các sự cố mất ATTT hay không?

43. Trong quá trình triển khai dự án phát triển ứng dụng CNTT, đơn vị có thực hiện tư vấn, thẩm định, thẩm tra về ATTTM của hệ thống thông tin được xây dựng hay không?

44. Tổng số lần đơn vị đã thực hiện kiểm tra đánh giá ATTTM định kỳ cho hệ thống thông tin của mình trong năm 2017 ?

45. Tổng số lần đơn vị đã tổ chức hoặc trực tiếp tham gia diễn tập bảo đảm ATTTM cho hệ thống thông tin của mình trong năm 2017 ?

46. Với các biện pháp kỹ thuật, công nghệ phù hợp đang được đơn vị đang áp dụng để bảo đảm ATTTM cho các HTTT nội bộ và HTTT công cộng, hãy cho biết lần trang bị, cập nhật, nâng cấp hay làm mới **gần đây nhất** là cách thời điểm hiện tại bao nhiêu tháng (tính cả tháng hiện tại) ?

Các biện pháp kỹ thuật, công nghệ bảo đảm an toàn mạng được trang bị, cập nhật, nâng cấp hay làm mới gần đây nhất cách hiện nay bao nhiêu tháng	**HTTT nội bộ**	**HTTT công cộng**
+ Hệ thống thiết bị sensor ghi log-file phát hiện sự cố và mối đe dọa ATTT đối với mạng		
+ Hệ thống giám sát và quản lý sự kiện an toàn thông tin (SOC-Security Operation Center / SIEM- Security Incident & Event Management)		
+ Giải pháp phân chia hệ thống mạng thành các vùng mạng chức năng với các chính sách quản lý và biện pháp kỹ thuật ATTTM phù hợp		
+ Hệ thống phát hiện xâm nhập (IDS/IPS) trong mạng		
+ Hệ thống phòng chống tấn công DoS/DDoS		
+ Tường lửa cho toàn mạng (Network Firewall)		
+ Phần mềm chống virus mức mạng (Anti-Virus)		
+ Bảo vệ kênh truyền bằng công nghệ mã hóa và xác thực		
+ Kiểm soát mọi kênh truy cập có bắt buộc định kỳ thay đổi mật khẩu người dùng		
+ Kiểm soát mọi kênh truy cập có giải pháp hạn chế đăng nhập tự động (tấn công kiểu từ điển) và/hoặc có yêu cầu xác thực hai yếu tố người dùng		
+ Bảo mật truy cập qua mạng không dây và các thiết bị đầu cuối		

47. Với các biện pháp kỹ thuật, công nghệ phù hợp đang được đơn vị áp dụng để bảo vệ các hệ thống máy chủ trong các HTTT nội bộ và HTTT công cộng, hãy cho biết lần trang bị, cập nhật, nâng cấp hay làm mới **gần đây nhất** là cách thời điểm hiện tại bao nhiêu tháng (tính cả tháng hiện tại) ?

Các công nghệ, biện pháp kỹ thuật bảo vệ các hệ thống máy chủ được trang bị, cập nhật, nâng cấp hay làm mới gần đây nhất cách hiện nay bao nhiêu tháng	**HTTT nội bộ**	**HTTT công cộng**
+ Hệ thống quản lý thu thập và phân tích log-file phát hiện sự cố và mối đe dọa ATTT		

+ Hệ thống phát hiện và chống tấn công xâm nhập máy chủ (IDS/IPS)		
+ Tường lửa (Firewall) cho máy chủ		
+ Phần mềm chống virus mã độc (Anti-Virus)		
+ Quản lý phân chia người dùng theo đặc quyền và có theo dõi phát hiện tài khoản người dùng lạ trong hệ thống		
+ Quản lý truy cập và chống tấn công leo thang đặc quyền		
+ Bảo mật thiết bị di động và thiết bị đầu cuối truy cập từ xa		
+ Sử dụng hệ thống máy chủ dự phòng nóng (chạy song song, on-line)		
+ Sử dụng hệ thống máy chủ dự trữ (dự phòng off-line)		

48. Với các biện pháp kỹ thuật, công nghệ phù hợp đang được đơn vị đang áp dụng để bảo vệ các ứng dụng trong các HTTT nội bộ và HTTT công cộng, hãy cho biết lần trang bị, cập nhật, nâng cấp hay làm mới gần đây nhất là cách thời điểm hiên tại bao nhiêu tháng (tính cả tháng hiện tại) ?

Các công nghệ, biện pháp kỹ thuật phù hợp bảo vệ các ứng dụng được trang bị, cập nhật, nâng cấp hay làm mới gần đây nhất cách hiện nay bao nhiêu tháng	**HTTT nội bộ**	**HTTT công cộng**
+ Hệ thống ghi nhật ký (log-file) các ứng dụng		
+ Hệ thống quản lý và phân tích log-file		
+ Quản lý truy cập có xác thực nhiều bước		
+ Phần mềm chống virus mã độc (Anti-Virus)		
+ Tường lửa mức ứng dụng (ví dụ web-firewall,...)		
+ Lọc nội dung Web		
+ Bộ lọc chống thư rác (Anti-Spam)		
+ Sử dụng hệ thống máy chủ dự phòng nóng (chạy song song, on-line)		
+ Sử dụng hệ thống máy chủ dự trữ (dự phòng off-line)		

49. Với các biện pháp kỹ thuật, công nghệ phù hợp đang được đơn vị đang áp dụng để bảo vệ dữ liệu cho các HTTT nội bộ và HTTT công cộng, hãy cho biết lần trang bị, cập nhật, nâng cấp hay làm mới **gần đây nhất** là cách thời điểm hiên tại bao nhiêu tháng (tính cả tháng hiện tại) ?

Các biện pháp kỹ thuật, công nghệ phù hợp bảo vệ dữ liệu được trang bị, cập nhật, nâng cấp hay làm mới gần đây nhất cách hiện nay bao nhiêu tháng	**HTTT nội bộ**	**HTTT công cộng**
+ Hệ thống giám sát tính toàn vẹn CSDL		
+ Hệ thống phát hiện xâm nhập CSDL		

+ Bảo vệ dữ liệu quan trọng trong hệ thống bằng công nghệ mã hóa		
+ Bảo vệ dữ liệu quan trọng trong hệ thống bằng công nghệ chữ ký số		
+ Hệ thống quản lý chống thất thoát dữ liệu (Data Loss protection)		
+ Sử dụng hệ thống sao lưu dữ liệu dự phòng nóng (on-line back-up)		
+ Sử dụng hệ thống sao lưu dữ liệu dự phòng định kỳ (off-line back-up)		

50. Với các biện pháp kỹ thuật, công nghệ phù hợp đang được đơn vị đang áp dụng để bảo đảm an toàn về mặt vật lý cho các HTTT nội bộ và HTTT công cộng, hãy cho biết lần trang bị, cập nhật, nâng cấp hay làm mới **gần đây nhất** là cách thời điểm hiện tại bao nhiêu tháng (tính cả tháng hiện tại) ?

Các biện pháp kỹ thuật, công nghệ phù hợp bảo đảm an toàn vật lý được trang bị, cập nhật, nâng cấp hay làm mới gần đây nhất cách thời điểm hiện tại bao nhiêu tháng	**HTTT nội bộ**	**HTTT công cộng**
+ Giải pháp lựa chọn vị trí vật lý		
+ Giải pháp kiểm soát truy cập vật lý		
+ Giải pháp chống trộm, chống phá hoại		
+ Giải pháp chống sét		
+ Hệ thống chống cháy nổ		
+ Giải pháp chống ẩm và chống thấm		
+ Giải pháp chống bụi và tĩnh điện		
+ Giải pháp kiểm soát nhiệt độ và độ ẩm		
+ Hệ thống nguồn cung cấp điện dự phòng		
+ Giải pháp bảo vệ điện từ trường		

51. Đơn vị có khả năng ghi nhận các hành vi tấn công (kể cả chưa thành công) vào hệ thống của mình hay không? | |

52. Khi hệ thống của đơn vị gặp sự cố mất ATTTM, quý vị sẽ báo cáo/thông báo tin này đi đâu? Đánh dấu tương ứng vào các ô phù hợp trong bảng sau:

Phản ứng / Loại sự cố, nguy cơ ATTTM	Tự xử lý, không báo cáo	Mời DN, sử dụng dịch vụ ngoài	Báo cáo cấp trên, ngành dọc	Báo và hợp tác với nhà mạng	Báo và hợp tác với đơn vị Bộ Quốc phòng	Báo và hợp tác với đơn vị Bộ Công an	Báo và hợp tác với đơn vị Bộ TTTT

Đơn vị đủ khả năng phát hiện và xử lý							
Đơn vị phát hiện được, chưa gây tác hại, nhưng khó xử lý							
Loại mới hoặc tấn công gây tác hại lớn, chưa tự xử lý được							

53. Từ 01/01/2017 đến hết 31/12/2017 đơn vị đã phát hiện được bao nhiêu sự cố ATTTM vào hệ thống của mình chưa gây ra thiệt hại hoặc gây ra thiệt hại nhỏ? Thống kê số vụ tấn công mạng đã xảy ra với các hệ thống thông tin do đơn vị quản lý (phân loại theo kiểu tấn công và hậu quả).

Số vụ tấn công mạng ít nghiêm trọng từ 01/01/2017 đến hết 31/12/2017	Số vụ tấn công web deface hay cài Phishing	Số lần tấn công từ chối dịch vụ (DDoS)	Số vụ tấn công bằng thư điện tử (spam)	Số máy tính trạm đã bị lây nhiễm mã độc	Số lần máy chủ bị tấn công bằng mã độc	Số vụ tấn công vào lỗ hổng ATTT của HTTT	Số sự cố khác (lỗi hạ tầng, vật lý, phần mềm)	Số vụ xâm nhập mạng do ATP, lộ mật khẩu
Số vụ đã phát hiện và ngăn chặn sớm, chưa gây ra thiệt hại								
Số vụ tấn công đã bị xâm nhập, lây nhiễm mã độc, nhưng chỉ gây ra thiệt hại nhỏ								

54. Số vụ tấn công, mất ATTTM nghiêm trọng (gây ra hậu quả nghiêm trọng về kinh tế, gián đoạn dịch vụ mạng, lộ lọt thông tin quan trọng...) xảy ra từ 01/01/2017 đến hết 31/12/2017

Số vụ việc mất ATTTM nghiêm trọng xảy ra từ	Số lần tấn công từ chối dịch vụ	Số lần máy chủ bị	Số máy tính trạm đã bị	Số vụ xâm nhập mạng do	Số vụ tấn công vào lỗ hổng	Số vụ tấn công web deface hay cài	Số vụ tấn công bằng thư	Số sự cố khác (lỗi hạ tầng,

01/01/2017 đến hết 31/12/2017	(DDoS)	tấn công bằng mã độc	lây nhiễm mã độc	ATP, lộ mật khẩu	ATTT của HTTT	Phishing	điện tử (spam -mail)	vật lý, phần mềm)
Tổng số vụ việc đã phát hiện, xử lý								
Đơn vị tự xử lý, khắc phục hậu quả thành công trong vòng 24h								
Được đơn vị khác hỗ trợ xử lý, khắc phục hậu quả thành công trong vòng 24h								

55. Theo quý vị những động cơ nào được nghi ngờ là nguyên nhân gây ra những hành động tấn công ở trên? (Có thể chọn nhiều đáp án là các mục sau)

Nhằm thể hiện kỹ năng tấn công	
Phá hoại hệ thống có chủ đích	
Nhằm chiếm dụng tài nguyên hệ thống để dẫn tới những cuộc tấn công nặc danh	
Thù hằn cá nhân (ví dụ: cán bộ hoặc người ngoài có thù hằn cá nhân)	
Nhằm tạo lợi thế cạnh tranh thương mại (ví dụ: tình báo công nghiệp)	
Chiếm đoạt tài nguyên hệ thống của cơ quan để sử dụng cho mục đích cá nhân	
Bị tấn công từ nước ngoài do các nguyên nhân liên quan đến chủ quyền	
Tạo nguồn thu tài chính bất hợp pháp	
Nhằm chiếm dụng tài nguyên hệ thống để dẫn tới những cuộc tấn công nặc danh	
Thù hằn cá nhân (ví dụ: cán bộ hoặc người ngoài có thù hằn cá nhân)	

56. Với tình hình hiện tại thì trong thời gian tới, đối tượng đe dọa tới ATTTM của hệ thống mà quý vị lo ngại nhất là gì ? (Ghi các số 1/2/3 tương ứng với các hạng mục lo ngại nhất, nhì và ba)

- Cán bộ đang làm việc tại công ty	
- Cán bộ đã nghỉ việc tại công ty	
- Tội phạm máy tính như *hacker* bất hợp pháp	
- Đối thủ cạnh tranh (*gián điệp công nghiệp*)	
- Băng nhóm tội phạm máy tính có tổ chức (*khủng bố mạng* v.v...)	
- Doanh nghiệp gia công bên ngoài (nhân viên) Outsourcing company (employees)	
- Các thế lực đến từ nước ngoài	
- Những mối đe dọa khác (vui lòng ghi rõ):	

57. Những vấn đề khó khăn nhất mà đơn vị gặp phải trong việc bảo đảm ATTTM cho hệ thống thông tin là gì? (Ghi các số 1/2/3/4/5 tương ứng với các hạng mục khó khăn nhất, nhì, ba, tư và năm)

Lãnh đạo chưa hỗ trợ đúng mức cần thiết cho ATTTM	
Sự thiếu hiểu biết về ATTTM trong đơn vị, thiếu cán bộ am hiểu kỹ thuật và quản lý ATTTM	
Việc nâng cao nhận thức và mặt bằng kiến thức cho người sử dụng máy tính về ATTTM	
Việc xác định chính xác mức độ ưu tiên của ATTTM trong tương quan chung với các vấn đề khác của đơn vị	
Việc áp dụng các nguyên tắc quản lý rủi ro (Risk Management principles) cho hệ thống thông tin	
Việc cập nhật kịp thời những cách thức tấn công hay những những điểm yếu mới xuất hiện	
Việc giám sát phát hiện, cảnh báo sớm các cuộc tấn công mạng	
Không đủ khả năng phản ứng nhanh và xử lý chính xác khi xảy ra những vụ tấn công qua mạng	
Việc quản lý chặt chẽ cấu hình hệ thống mạng (Configuration Management)	
Những hệ thống máy tính không được quản lý tốt	
Kinh phí/ngân sách dành cho ATTTM quá thiếu so với mặt bằng chung	
Các vấn đề khác (Nếu có thì vui lòng ghi rõ):	

58. Số lần đơn vị đã rút kinh nghiệm bài học khắc phục sự cố dẫn đến việc thay đổi, bổ sung, hoàn thiện quy định, quy chế ứng cứu sự cố và bảo đảm ATTTM trong năm 2017 | |

59. Đơn vị có sử dụng chữ ký số để bảo đảm an toàn cho các giao dịch điện tử hay không? | |

Lãnh đạo đơn vị
(Ký, ghi rõ họ tên và đóng dấu)

Người lập bảng khảo sát

Họ tên:.....

Điện thoại:.....

Email:.....

Báo cáo đã điền đầy đủ nội dung xin gửi đơn vị đầu mối của cơ quan để tổng hợp, sau đó gửi về Cục An toàn thông tin, Bộ Thông tin và Truyền thông, địa chỉ: tầng 8, số 115 Trần Duy Hưng, Hà Nội.

Mẫu số 03

Bảng tổng hợp danh mục báo cáo

(Kèm theo công văn số /BTTTT-CATTT ngày /02/2018)

Tên cơ quan báo cáo:.....

Stt	Tên đơn vị	Tên file bản mềm	Ghi chú
1	Tên cơ quan	01	
2	Cục A	02	
3	Cục B	03	
.....	.....	.....	

Lãnh đạo cơ quan
(Ký, ghi rõ họ tên và đóng dấu)

Người lập

Họ tên:.....

Điện thoại:.....

Email:.....

Hướng dẫn thực hiện báo cáo hoạt động bảo đảm an toàn thông tin mạng

(Kèm theo công văn số 481 /BTTTT-CATTT ngày 12 /02/2018)

1. Đối tượng đánh giá

Các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương (sau đây gọi tắt là cơ quan).

2. Mục tiêu đánh giá

- Đánh giá mức độ bảo đảm an toàn thông tin mạng của các cơ quan để phục vụ công tác quản lý nhà nước về an toàn thông tin và đánh giá khả năng bảo đảm an toàn thông tin của cơ quan trong triển khai xây dựng Chính phủ điện tử.

- Giúp các cơ quan biết được mức độ bảo đảm an toàn thông tin mạng của cơ quan mình, từ đó đưa ra các biện pháp phù hợp nhằm bảo đảm an toàn thông tin trong quá trình ứng dụng CNTT cũng như xây dựng Chính phủ điện tử.

3. Phạm vi thực hiện

Để có thể đánh giá được mức độ bảo đảm an toàn thông tin mạng thì số liệu sẽ được tổng hợp từ báo cáo của các cơ quan. Phạm vi báo cáo của các cơ quan được phân chia thành 02 cấp là cấp cơ quan và cấp đơn vị với cách hiểu các thuật ngữ như sau:

- **Cơ quan** (hoặc cơ quan chủ quản trong Mẫu báo cáo của đơn vị trực thuộc): chỉ các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, UBND tỉnh/thành phố trực thuộc TW.

- **Đơn vị:** chỉ các đơn vị trực thuộc trực tiếp các cơ quan. Phạm vi bao gồm:

+ Các văn phòng, vụ, tổng cục, cục, viện, Ban quản lý, quỹ, đơn vị sự nghiệp công lập hoặc các đơn vị tương đương khác trực thuộc trực tiếp các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ.

+ Các thành phố, văn phòng, sở, quận, huyện, Ban quản lý, quỹ, đơn vị sự nghiệp công lập hoặc các đơn vị tương đương khác trực thuộc trực tiếp UBND các tỉnh, thành phố trực thuộc TW.

Lưu ý: *Trường hợp một số đơn vị không trực tiếp quản lý, vận hành hệ thống thông tin thì không bắt buộc phải thực hiện riêng mẫu báo cáo mà có thể gộp trong báo cáo của đơn vị quản lý, vận hành hệ thống thông tin.*

Ví dụ: Vụ A của Bộ B không trực tiếp quản lý, vận hành hệ thống thông tin riêng biệt mà chỉ có mạng LAN phục vụ cho các máy tính của người sử dụng và

được quản lý, vận hành chung bởi Văn phòng Bộ B thì có thể gộp các số liệu của Vụ A vào trong báo cáo của Văn phòng Bộ B.

4. Phương thức thực hiện

4.1. Mẫu báo cáo

Đơn vị đầu mối tải các mẫu báo cáo từ địa chỉ https://ais.gov.vn, bao gồm:

- Mẫu số 01 (bản word và bản excel): là mẫu báo cáo cấp cơ quan, áp dụng cho các hệ thống thông tin và hoạt động bảo đảm an toàn thông tin mạng cấp cơ quan. Ví dụ: các hệ thống thông tin dùng chung cho nội bộ hoặc công công của một bộ, UBND như: cổng thông tin điện tử, hệ thống cung cấp dịch vụ công trực tuyến.

Lưu ý: các số liệu, thông tin của cấp cơ quan được tổng hợp bình thường giống như cấp đơn vị trực thuộc, không phải là số liệu được cộng dồn từ báo cáo của các đơn vị trực thuộc.

- Mẫu số 02 (bản word và bản excel): là mẫu báo cáo để đơn vị đầu mối gửi cho các đơn vị trực thuộc trực tiếp cơ quan điền thông tin.

4.2. Phân công thực hiện báo cáo

Đối với mỗi cơ quan: thực hiện tổng hợp thông tin, số liệu tổng thể và thông tin, số liệu đối với từng đơn vị trực thuộc. Cụ thể:

- Báo cáo theo Mẫu số 01: do đơn vị chuyên trách về an toàn thông tin/công nghệ thông tin (ATTT/CNTT) hoặc đơn vị được giao làm đầu mối (gọi tắt là đơn vị đầu mối) của cơ quan thực hiện điền thông tin.

- Báo cáo theo Mẫu số 02: do các đơn vị trực thuộc trực tiếp của cơ quan thực hiện điền thông tin theo hướng dẫn của đơn vị đầu mối.

Ngoài Mẫu số 01, đơn vị đầu mối vẫn phải thực hiện Mẫu số 02 của mình như một đơn vị bình thường.

4.3. Hướng dẫn triển khai

Việc thực hiện báo cáo hoạt động bảo đảm an toàn thông tin mạng của mỗi cơ quan có thể được triển khai theo 4 bước gợi ý như sau:

- Bước 1: Lãnh đạo cơ quan giao cho đơn vị đầu mối tổ chức triển khai.

- Bước 2: Đơn vị đầu mối tải các mẫu báo cáo và hướng dẫn chi tiết, gửi cho các đơn vị điền mẫu báo cáo (bản cứng và bản mềm excel). Hướng dẫn thắc mắc cho các đơn vị trong quá trình thực hiện.

- Bước 3: Các đơn vị điền thông tin vào mẫu báo cáo (bản cứng và bản mềm excel) và gửi lại cho đơn vị đầu mối.

- Bước 4: Đơn vị đầu mối tổng hợp hồ sơ, trình lãnh đạo cơ quan để gửi báo cáo về Bộ Thông tin và Truyền thông theo địa chỉ được nêu trong công văn. Hồ sơ gửi Bộ Thông tin và Truyền thông gồm các nội dung như mục 4.4 dưới đây.

4.4. Hồ sơ báo cáo gửi Bộ Thông tin và Truyền thông

Hồ sơ báo cáo của các cơ quan gửi về Bộ Thông tin và Truyền thông bao gồm:

- Văn bản của cơ quan;

- Bản cứng các báo cáo đã được điền đầy đủ thông tin, bao gồm: 01 bản theo Mẫu số 01 và các báo cáo theo Mẫu số 02 của các đơn vị.

- Bản mềm các báo cáo (excel): tương ứng với các bản cứng nêu trên, gửi về địa chỉ thư điện tử: tdkhoa@mic.gov.vn.

Lưu ý: Tên file đặt theo hướng dẫn tại mẫu số 03 kèm theo công văn.

- Bảng tổng hợp danh mục báo cáo: theo mẫu số 03 kèm theo công văn.

5. Hướng dẫn thực hiện

Trong quá trình thực hiện, nếu có thắc mắc, các đơn vị liên hệ đơn vị đầu mối để được hướng dẫn thực hiện.

Trường hợp đơn vị đầu mối có thắc mắc hoặc các nội dung khó mà đơn vị đầu mối chưa xử lý dứt điểm được, các đơn vị có thể liên hệ Cục An toàn thông tin (Bộ Thông tin và Truyền thông) để được hướng dẫn theo thông tin liên hệ như sau:

Ông Trần Đăng Khoa, Phó Trưởng phòng phụ trách, Cục An toàn thông tin, Bộ Thông tin và Truyền thông, thư điện tử: tdkhoa@mic.gov.vn, điện thoại: 0904804803./.