Ký bởi Ủy ban Nhân dân huyện Nga Sơn
Tỉnh Thanh Hóa
ngason@thanhhoa.gov.vn
Giờ ký: 2020-03-31T17:26:39.8641964+07:00

ỦY BAN NHÂN DÂN **HUYỆN NGA SƠN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 440/UBND-VH V/v báo cáo đánh giá mức độ bảo đảm an toàn thông tin mạng huyện Nga Sơn .	*Nga Sơn, ngày 31 tháng 3 năm 2020*

Kính gửi: Sở Thông tin và Truyền thông tỉnh Thanh Hóa.

Thực hiện Công văn số 422/STTTT-CNTT ngày 23/3/2020 của Sở Thông tin và Truyền thông tỉnh Thanh Hóa về việc đánh giá mức độ bảo đảm an toàn thông tin mạng của cơ quan, đơn vị trên địa bàn tỉnh Thanh Hóa.

UBND huyện báo cáo đánh giá mức độ bảo đảm an toàn thông tin mạng trên địa bàn như sau:

(Phụ lục báo cáo kèm theo)

UBND huyện Nga Sơn trân trọng báo cáo./.

Nơi nhận:
- Như trên (BC);
- Văn phòng UBND&UBND huyện;
- Phòng Văn hóa và Thông tin;
- Lưu: VT.

KT.CHỦ TỊCH
PHÓ CHỦ TỊCH

ỦY BAN NHÂN DÂN HUYỆN NGA SƠN T. THANH HÓA

Mai Đình Hiếu

MẪU BÁO CÁO SỐ 2: PHỤC VỤ ĐÁNH GIÁ MỨC ĐỘ ATTT MẠNG 2019
ĐỐI TƯỢNG: SỞ BAN NGÀNH, UBND HUYỆN, THỊ XÃ, THÀNH PHỐ

A. Thông tin chung

1

Tên đơn vị báo cáo:	UBND huyện Nga Sơn
Trực thuộc:	Tỉnh Thanh Hóa

2 Đề nghị thống kê số lượng các hệ thống thông tin Quý cơ quan đã xác định và phê duyệt cấp độ:

Phân loại số lượng HTTT do đơn vị được giao quản lý	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)				1		
Số **HTTT công cộng** (có người ngoài đơn vị sử dụng)						

Văn bản tham chiếu (Số QĐ/ngày ký)
330/QĐ-UBND ngày 20/01/2020 Về việc

3 Quý đơn vị cung cấp **bao nhiêu dịch vụ độc lập (trọn gói)** sử dụng phục vụ cộng đồng trên mạng internet? | 350 |

B. Khảo sát môi trường An toàn thông tin mạng

I. Chính sách ATTTM

4 Đơn vị có ban hành quy định riêng hoặc có áp dụng quy chế chung về bảo đảm ATTTM không? | 0 |

Loại văn bản chính sách ATTTM được Quý đơn vị áp dụng	Văn bản hiện hành		Văn bản cũ đã được thay thế bằng VB hiện hành (nếu có)	
	Năm	Số VB/Quyết định	Năm	Số VB/ Quyết định
Quy định riêng				
Quy chế chung				
Văn bản QĐ áp dụng quy chế				
...				

5 Trong các quy định hiện hành về bảo đảm ATTTM của Quý đơn vị có bao gồm các nội dung nào sau đây?

Các nội dung quản lý nào có trong quy định hiện hành ?	
Quản lý thiết kế, xây dựng an toàn HTTT	
Quản lý vận hành an toàn HTTT	
Quản lý phát triển nhân lực ATTT và người sử dụng HTTT	

Quản lý rủi ro về ATTTM	
Quản lý sự cố ATTTM	

6 Đề nghị tự nhận xét về chất lượng của bộ quy định/quy chế hiện hành so với yêu cầu của Quý đơn vị đến thời điểm hiện nay?

+ 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 Đề nghị tự đánh giá thực tế hiện nay tại đơn vị, mức độ áp dụng thực hiện tốt các quy chế, quy định bảo đảm ATTTM đạt khoảng độ bao nhiêu phần trăm?

II. Tổ chức và quản lý nhân lực bảo đảm ATTTM

8	Đơn vị có phân công lãnh đạo phụ trách về ATTT.	0	Nội dung tham chiếu
9	Tổng số cán bộ nhân viên nói chung làm việc trong đơn vị.	104	
10	Số người sử dụng máy tính hiện tại.	104	
11	Có tổ chức/bộ phận chuyên trách về ATTTM hay không?	1	Nội dung tham chiếu

Là bộ phận con thuộc tổ chức phụ trách CNTT của đơn vị ?	1
Chịu sự chỉ đạo nghiệp vụ của bộ phận chuyên trách ATTTM cấp trên,…?	1
Là thành viên thuộc mạng lưới Ứng cứu khẩn cấp máy tính quốc gia?	1

12 Vị trí và quan hệ công tác của bộ phận chịu trách nhiệm về ATTTM.

Có cơ chế và đầu mối liên hệ phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý/ điều phối ứng cứu về ATTTM	1
Có cơ chế và đầu mối liên hệ phối hợp bảo đảm ATTTM với các tổ chức, doanh nghiệp liên quan? Ví dụ: với các DN cung cấp dịch vụ mạng, dịch vụ ATTT	1

13 Số cán bộ làm việc chuyên trách và bán chuyên trách ATTTM?

- Số chuyên trách	1
- Số bán chuyên	0

14 Quản lý nhân sự phù hợp với yêu cầu ATTT như thế nào? Có quy định từng khâu? Thực hiện được ở mức nào?

Các khâu quản lý	Tuyển dụng cán bộ phù	Quản lý quá trình làm	Thủ tục ATTT khi chấm dứt	
Chưa ban hành quy chế hay quy định cụ thể/ Không chú ý.				Nội dung tham chiếu
Chưa ban hành quy định cụ thể nhưng có thực hiện quản lý theo kinh nghiệm.				Nội dung tham chiếu
Có quy định nhưng thực hiện chưa thường xuyên.				Nội dung tham chiếu

Có quy định và thực hiện tốt.				Nội dung tham chiếu

III. Trình độ, nhận thức và đào tạo bồi dưỡng về ATTT

15	a. Tổng số cán bộ nhân viên đã từng được hướng dẫn kỹ năng cơ bản để tự bảo đảm ATTT.	1	Nội dung tham chiếu
	b. Tổng số cán bộ nhân viên đã từng được qua lớp tập huấn về ATTM.	1	Nội dung tham chiếu
16	a. Tổng số cán bộ kỹ thuật về ATTT, CNTT của đơn vị	1	Nội dung tham chiếu
	b. Tổng số cán bộ kỹ thuật về ATTT, CNTT của đơn vị được đào tạo, tập huấn, nâng cao nhận thức về ATTM	1	Nội dung tham chiếu
17	Tổng số cán bộ kỹ thuật có trình độ tương đương đại học ngành ATTT trở lên.	1	Nội dung tham chiếu
18	Tổng số cán bộ kỹ thuật có trình độ tương đương trung cấp về ATTT.	1	Nội dung tham chiếu
19	Đơn vị có kế hoạch đào tạo, tập huấn riêng về ATTTM trong năm 2019 hay không ?	0	Nội dung tham chiếu
20	Quý đơn vị có thực hiện kế hoạch riêng tuyên truyền, phổ biến nâng cao nhận thức về ATTTM trong năm 2019 hay không?	1	Nội dung tham chiếu

IV. Về tổ chức triển khai bảo đảm ATTTM

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

+ Chủ trương không thuê ngoài dịch vụ bảo đảm ATTTM.	1
+ Có chủ trương (thuê/không thuê) nhưng chưa thực hiện đúng được.	
+ Chủ trương có thuê và đã thuê ngoài dịch vụ bảo đảm ATTTM mỗi khi cần.	

22 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

+ Chủ trương không thuê.	1
+ Có chủ trương nhưng chưa thực hiện đúng được.	
+ Chủ trương có thuê và đang thuê dịch vụ của các công ty Việt Nam không có yếu tố nước ngoài.	

23 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

+ Chủ trương không sử dụng dịch vụ này.	1
+ Chủ trương có thuê nhưng chưa sử dụng dịch vụ này.	
+ Đang sử dụng loại dịch vụ này (dù có hay không có chủ trương).	

24 Đơn vị bảo đảm ATTTM thường xuyên bằng cách nào?

+ Hoàn toàn sử dụng nội lực.	1
+ Sử dụng toàn bộ thuê và hỗ trợ từ bên ngoài.	
+ Sử dụng một phần nội lực một phần lực lượng bên ngoài.	

V. Bố trí kinh phí

25 Kinh phí dành cho CNTT và ATTT trong 3 năm qua (triệu đồng).

Kinh phí \ Năm	2017	2018	2019
Dành cho CNTT			
Dành cho ATTT			

26 Ước tính toàn bộ chi phí về ATTTM trong 3 năm qua đáp ứng bao nhiêu % nhu cầu (dự toán) của đơn vị?

Mức đáp ứng nhu cầu chi hàng	2017	2018	2019
Đáp ứng dưới 20%			
Đáp ứng từ 20% đến 50%			
Đáp ứng từ 51% đến 75%			
Đáp ứng trên 75%			

C. Khảo sát các biện pháp được áp dụng và kết quả hoạt động thực tiễn trong năm 2019

VI. Biện pháp quản lý

27	a. Đơn vị đã triển khai bảo đảm an toàn hệ thống thông tin theo cấp độ đáp ứng Thông tư số 03/2017/TT-BTTTT chưa?		Nội dung tham chiếu
	b. Đơn vị có triển khai thực hiện tiêu chuẩn TCVN 11930:2017 về bảo đảm an toàn hệ thống thông tin theo cấp độ không?		Nội dung tham chiếu
28	Đơn vị đã nhận chứng nhận hợp chuẩn quản lý ATTTM theo tiêu chuẩn trên chưa?		Nội dung tham chiếu

Thời điểm hợp chuẩn cách đây bao nhiêu tháng?

Tiêu chuẩn \ Thời gian	cho lần đầu tiên (số tháng)	lần cuối - mới nhất (số tháng)
TCVN/ISO-IEC 27001 (hay tương tự)		
TCVN 11930:2017		

29	Việc quản lý cán bộ vận hành, khai thác, sử dụng hệ thống của đơn vị có tuân thủ các chính sách về ATTT hay không?	1
30	Đơn vị có sử dụng chữ ký số để bảo đảm an toàn cho các giao dịch điện tử hay không?	1
31	Đơn vị có ban hành quy trình thao tác chuẩn để phản ứng với các sự cố mất ATTT hay không?	0

- Đánh giá mức độ thực hiện một số biện pháp quản lý ATTTM quan trọng cho HTTT

32 Quản lý thiết kế, xây dựng hệ thống trong năm 2019:

a) Trong năm nay đơn vị có thiết kế/xây dựng HTTT mới không?		0
- Có quản lý và bảo vệ tài liệu hồ sơ thiết kế HTTT.		
- Có phương án và giải pháp bảo đảm ATTTM cho HTTT từ khi thiết kế.		
- Thẩm định hồ sơ thiết kế và các biện pháp bảo đảm ATTT trước khi triển khai thực hiện.		
b) Trong năm nay đơn vị có thuê ngoài phát triển phần mềm nội bộ (phát triển riêng) cho mình không?		
- Quản lý tốt hồ sơ hợp đồng, thử nghiệm, nghiệm thu và mã nguồn phần mềm.		

- Có kiểm tra, đánh giá an toàn thông tin HT phần mềm trước khi đưa vào sử dụng.	
- Có cam kết của nhà phát triển bảo đảm bí mật và bản quyền của phần mềm.	

c) Trong năm nay đơn vị có đưa vào sử dụng HTTT mới hay mới được nâng cấp không?

- Thực hiện quy trình thử nghiệm, nghiệm thu HTTT trước khi bàn giao sử dụng.	
- Có tư vấn và giám sát độc lập khâu thử nghiệm và nghiệm thu HTTT.	
- Báo cáo nghiệm thu HTTT có được xác nhận của bộ phận chuyên trách và phê duyệt của lãnh đạo trước khi đưa vào sử dụng	
- Kiểm tra, đánh giá ATTT trước khi đưa vào vận hành.	

33 Đánh giá quản lý vận hành ATTT cho HTTT trong năm 2019

a) Thực hiện tốt các nội dung nào về quản lý vận hành an toàn mạng?

- Quản lý các khâu vận hành, cập nhật, sao lưu dự phòng hoạt động hệ thống.	1
- Quản lý cấu hình, tối ưu hóa bảo mật cho thiết bị hệ thống.	1
- Khôi phục hệ thống mạng sau khi xảy ra sự cố.	1

b) Thực hiện tốt các nội dung nào về quản lý vận hành máy chủ và ứng dụng?

- Quản lý, vận hành, truy cập mạng và quản trị máy chủ và dịch vụ; Cập nhật, sao lưu dự phòng.	1
- Quản lý cài đặt, gỡ bỏ phần mềm, dịch vụ trên máy chủ; Quản lý kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống.	1
- Quản lý cấu hình, tối ưu hóa bảo mật cho hệ thống máy chủ, phòng ngừa và khôi phục sau khi xảy ra sự cố.	1

c) Thực hiện tốt các nội dung nào về quản lý an toàn dữ liệu?

- Quy trình áp dụng mã hóa, quản lý và sử dụng khóa bí mật và dữ liệu mã hóa.	
- Cơ chế kiểm tra tính nguyên vẹn của dữ liệu trong lưu trữ và trao đổi dữ liệu.	
- Sao lưu dự phòng và khôi phục dữ liệu; Cập nhật đồng bộ dữ liệu.	

d) Thực hiện tốt các nội dung nào về quản lý vận hành an toàn thiết bị đầu cuối?

- Quản lý, vận hành hoạt động; Cấu hình tối ưu và tăng cường bảo mật cho thiết bị đầu cuối.	1
- Quản lý truy cập của thiết bị đầu cuối; Cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống.	1
- Quản lý kiểm tra, xử lý điểm yếu an toàn thông tin cho thiết bị đầu cuối trước khi sử dụng.	1

đ) Thực hiện tốt các nội dung nào về quản lý phòng chống phần mềm độc hại?

- Quy trình cài đặt, cập nhật, sử dụng phần mềm phòng chống mã độc trong hệ thống; Cài đặt, sử dụng phần mềm trên máy tính, thiết bị di động	
- Truy cập các trang thông tin trên mạng; Gửi nhận tập tin qua môi trường mạng và các phương tiện lưu trữ di động.	
- Thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống	

e) Thực hiện tốt các nội dung nào về quản lý an toàn người sử dụng đầu cuối?

- Có quy trình quản lý truy cập, sử dụng tài nguyên nội bộ.	1
- Có quy trình quản lý truy cập mạng và tài nguyên trên Internet.	1
- Có quy trình cài đặt và sử dụng máy tính an toàn.	1

34 Các biện pháp quản lý rủi ro ATTT, giám sát và quản lý ứng cứu sự cố ATTT.

a) Thực hiện tốt các nội dung nào về quản lý rủi ro ATTT?

- Thực hiện phân loại, xác định giá trị và trách nhiệm về sở hữu tài sản thông tin trong hệ thống.	
- Phân tích đánh giá nguy cơ thực tế mất ATTT và dự kiến thiệt hại với HTTT. Từ đó đề xuất, lựa chọn phương án xử lý rủi ro ATTT và các biện pháp khắc phục sự cố với chi phí tối ưu, tối thiểu hóa giá trị thiệt hại với nguồn lực hiện có.	
- Thực hiện kiểm tra đánh giá và thông qua diễn tập định kỳ và thực tiễn khắc phục sự cố để đào tạo đội ngũ nhân lực, rút kinh nghiệm và cải tiến phương án xử lý rủi ro, bảo đảm ATTTM.	

b) Thực hiện tốt các nội dung nào về quản lý giám sát an toàn HTTT?

- Có kế hoạch giám sát phát hiện nguy cơ mất ATTT: Quản lý, vận hành hệ thống giám sát; Quản lý đối tượng giám sát, quản trị hệ thống giám sát, quản lý nhật ký hệ thống.	
- Tổ chức giám sát an toàn cho HTTT liên tục 24/7 có đồng bộ thời gian HTTT với hệ thống giám sát.	
- Thu thập, lưu trữ và bảo vệ thông tin giám sát; Theo dõi, phân tích kết quả giám sát.	
- Phát cảnh báo sự cố phát hiện được, trao đổi chia sẻ thông tin cảnh báo và sự cố theo quy định.	

- HTTT của đơn vị được giám sát ATTT bằng cách nào?

* Tự thực hiện giám sát do đã đầu tư hệ thống kỹ thuật.	
* Thuê dịch vụ giám sát của tổ chức, doanh nghiệp.	
Trường hợp đang thuê, hãy nêu tên của tổ chức, doanh nghiệp đang cung cấp dịch vụ:	

c) Thực hiện tốt các nội dung nào về quản lý điểm yếu ATTT ?

- Quản lý, cập nhật danh mục điểm yếu ATTT liên quan đến các thành phần của HTTT.	
- Có cơ chế phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu ATTT.	
- Kiểm tra, đánh giá và xử lý điểm yếu ATTT cho HTTT, máy chủ, dịch vụ trước khi đưa vào sử dụng hoặc khi có thông tin cảnh báo; Có phương án xử lý tạm thời khi điểm yếu ATTT không/chưa có khả năng khắc phục.	
- Có quy trình khôi phục lại hệ thống sau khi xử lý điểm yếu ATTT thất bại.	

d) Thực hiện tốt các nội dung nào về quản lý ứng cứu sự cố ATTT?

- Có quy trình phát hiện, tiếp nhận cảnh báo, nhận dạng và phân loại sự cố ATTT.	
- Có quy trình xử lý khẩn cấp ban đầu phù hợp với các loại sự cố có thể xảy ra, hạn chế thiệt hại nhanh nhất có thể.	
- Có quy định chia sẻ thông tin, báo cáo sự cố, điều phối ứng cứu sự cố. Có cơ chế phối hợp với cơ quan chức năng, các chuyên gia, bên cung cấp dịch vụ hỗ trợ trong xử lý, khắc phục sự cố.	
- Có quy trình ứng cứu sự cố ATTT thông thường và sự cố ATTT nghiêm trọng.	
- Thực hiện các bước khôi phục hệ thống, dữ liệu, dịch vụ, khắc phục thiệt hại.	
- Định kỳ thường xuyên tổ chức diễn tập phản ứng khẩn cấp với sự cố ATTTM.	
- Định kỳ đánh giá hiệu quả và hoàn thiện các quy định, quy trình thao tác chuẩn phản ứng với sự cố.	

VII. Biện pháp kỹ thuật, công nghệ đang áp dụng

35 Các biện pháp kỹ thuật, công nghệ phù hợp **bảo đảm an toàn mạng** nào đang được sử dụng cho các HTTT nội bộ và HTTT công cộng? Lần làm mới gần đây nhất là mm-yyyy khi nào?

Các biện pháp kỹ thuật, công nghệ bảo đảm an toàn mạng đang được sử dụng	**HTTT nội bộ**	**HTTT công cộng**	Nội dung tham chiếu (Tên giải pháp, phiên bản sử dụng..)
+ Hệ thống thiết bị sensor ghi log-file phát hiện sự cố và mối đe dọa ATTT đối với mạng.			
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).	1		
+ 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.			
thực hai yếu tố người dùng.			
+ Bảo mật truy cập qua mạng không dây và các thiết bị đầu cuối.	1		

36 Các biện pháp kỹ thuật, công nghệ được áp dụng để **bảo vệ các hệ thống máy chủ** trong các HTTT nội bộ và HTTT công cộng? Lần làm mới gần đây nhất là khi nào mm-yyyy?

Các công nghệ, biện pháp kỹ thuật bảo vệ các hệ thống máy chủ đang được sử dụng	**HTTT nội bộ**	**HTTT công cộng**	Nội dung tham chiếu (Tên giải pháp, phiên bản sử dụng..)
+ 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).			

37 Các biện pháp kỹ thuật, công nghệ đang được áp dụng để **bảo vệ các ứng dụng** trong các HTTT nội bộ và HTTT công cộng?
Lần làm mới gần đây nhất là khi nào mm-yyyy?

Các công nghệ, biện pháp kỹ thuật phù hợp bảo vệ các ứng dụng đang được sử dụng	**HTTT nội bộ**	**HTTT công cộng**	Nội dung tham chiếu (Tên giải pháp, phiên bản sử dụng..)
+ 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).			

38 Các biện pháp kỹ thuật, công nghệ phù hợp đang được áp dụng để **bảo vệ dữ liệu** cho các HTTT nội bộ và HTTT công cộng?
Lần làm mới gần đây nhất là khi nào mm-yyyy?

Các biện pháp kỹ thuật, công nghệ phù hợp bảo vệ dữ liệu đang được sử dụng	**HTTT nội bộ**	**HTTT công cộng**	Nội dung tham chiếu (Tên giải pháp, phiên bản sử dụng..)
+ 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)			

39 Các biện pháp kỹ thuật, công nghệ phù hợp đang được áp dụng để **bảo đảm an toàn về mặt vật lý** cho các HTTT nội bộ và HTTT công cộng? Lần làm mới gần đây nhất là khi nào mm-yyyy?

Các biện pháp kỹ thuật, công nghệ phù hợp bảo đảm an toàn vật lý đang được sử dụng	**HTTT nội bộ**	**HTTT công cộng**	Nội dung tham chiếu
+ Giải pháp lựa chọn vị trí vật lý.	0		
+ Giải pháp kiểm soát truy cập vật lý.	0		
+ Giải pháp chống trộm, chống phá hoại .	0		
+ Giải pháp chống sét.	0		
+ 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.			

VIII. Hoạt động thực tiễn năm 2019

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

41 Khi hệ thống của đơn vị gặp sự cố mất ATTTM, quý vị đã báo cáo/thông báo tin này đi đâu?

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 & hợp tác với DN DV mạng	Báo và hợp tác với đơn vị Bộ QP	Báo và hợp tác với đơn vị 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			1	1			
Loại mới hoặc tấn công gây tác hại lớn, chưa tự xử lý được							

42 Trong năm 2019 đơn vị đã phát hiện được bao nhiêu vụ việc mất ATTTM nhưng chưa gây ra thiệt hại hoặc chỉ gây ra thiệt hại nhỏ?

Số sự cố ATTTM ít nghiêm trọng năm 2019	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-mail)	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.	0	0	0	0	0	0	0	0
Số vụ tấn công đã bị xâm nhập, lây nhiễm mã độc, nhưng chỉ gây ra thiệt hại nhỏ.	0	0	0	7	0	0	0	0

43 Số vụ tấn công, mất ATTTM nghiêm trọng (gây ra hậu quả lớn về kinh tế, gián đoạn dịch vụ mạng, lộ lọt thông tin quan trọng…) đã xảy ra

Số vụ việc mất ATTTM nghiêm trọng xảy ra trong năm qua	Số lần tấn công từ chối dịch vụ (DDoS)	Số lần máy chủ bị tấn công bằng mã độc	Số máy tính trạm đã bị lây nhiễm mã độc	Số vụ xâm nhập mạng do ATP, lộ mật khẩu	Số vụ tấn công vào lỗ hổng ATTT của HTTT	Số vụ tấn công web deface hay cài Phishing	Số vụ tấn công bằng thư điện tử (spam-mail)	Số sự cố khác (lỗi hạ tầng, vật lý, phần mềm)
Tổng số vụ việc đã phát hiện, xử lý	0	0	0	0	0	0	0	0
Đơn vị tự xử lý, khắc phục hậu quả thành công trong vòng 24h	0	0	0	0	0	0	0	0
Được đơn vị khác hỗ trợ xử lý, khắc phục hậu quả thành công trong vòng 24h	0	0	0	0	0	0	0	0

44 Theo quý đơn vị những động cơ nào được nghi ngờ là nguyên nhân gây ra những hành động tấn công ở trên?

Nhằm thể hiện kỹ năng tấn công.	
Phá hoại hệ thống có chủ đích.	1
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.	1
Bị tấn công từ nước ngoài do các nguyên nhân liên quan đến chủ quyền.	

Tạo nguồn thu tài chính bất hợp pháp.	

45 Với tình hình hiện tại thì trong thời gian tới, đối tượng đe dọa tới ATTTM của hệ thống mà quý đơn vị lo ngại nhất là gì ? (Ghi các số 1/2/3

- Cán bộ đang làm việc tại đơn vị.	1
- Cán bộ đã nghỉ việc tại đơn vị.	1
- Tội phạm máy tính như *hacker* bất hợp pháp.	1
- Đối thủ cạnh tranh (*gián điệp công nghiệp*).	1
- Băng nhóm tội phạm máy tính có tổ chức (*khủng bố mạng* v.v...).	1
- Doanh nghiệp gia công bên ngoài (nhân viên) Outsourcing company (employees).	1
- Các thế lực đến từ nước ngoài.	1
- Những mối đe dọa khác (vui lòng ghi rõ vào hai ô dưới):	1

46 Những vấn đề khó khăn nhất mà đơn vị gặp phải trong việc bảo đảm ATTTM cho HTTT là gì? (Ghi các số 1/2/3 tương ứng với các hạng mục

Lãnh đạo chưa hỗ trợ đúng mức cần thiết cho ATTTM.	1
Sự thiếu hiểu biết về ATTTM trong đơn vị, thiếu cán bộ am hiểu kỹ thuật và quản lý ATTTM.	1
Việc nâng cao nhận thức và mặt bằng kiến thức cho người sử dụng máy tính về ATTTM.	1
Việc xác định đúng mức độ ưu tiên của ATTTM trong tương quan chung với các vấn đề khác của đơn vị.	1
Việc áp dụng đúng các nguyên tắc quản lý rủi ro (Risk Management principles) cho hệ thống thông tin.	1
Việc cập nhật kịp thời những cách thức tấn công hay những những điểm yếu mới xuất hiện.	1
Việc giám sát phát hiện, cảnh báo sớm các cuộc tấn công mạng.	1
Không đủ khả năng phản ứng nhanh và xử lý chính xác khi xảy ra những vụ tấn công qua mạng.	1
Việc quản lý chặt chẽ cấu hình hệ thống mạng (Configuration Management).	1
Những hệ thống máy tính không được quản lý tốt.	1
Kinh phí/ngân sách danh cho ATTTM quá thiếu so với mặt bằng chung.	1
Các vấn đề khác (vui lòng ghi rõ vào hai ô dưới):	1

47	Tổng số lần đơn vị đã thực hiện kiểm tra đánh giá ATTTM định kỳ cho HTTT của mình trong năm 2019?		Nội dung tham chiếu
48	Trường hợp cơ quan đánh giá ATTTM định kỳ là tự thực hiện hay thuê dịch vụ đơn vị độc lập?		Nội dung tham chiếu
49	Tổng số lần đơn vị đã tổ chức hay tham gia diễn tập bảo đảm ATTTM cho HTTT của mình trong năm 2019?	0	Nội dung tham chiếu

50	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 qua?	0

THÔNG TIN NGƯỜI ĐIỀN PHIẾU

Họ và tên	Phạm Văn Lưu
Bộ phận công tác	Văn phòng HĐND&UBND huyện Nga Sơn
Chức vụ	viên chức biệt phái
Điện thoại di động	
Email	

Nga Sơn,ngày 30 tháng 3 năm 2020

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH TT

ỦY BAN NHÂN DÂN HUYỆN NGA SƠN T. THANH HÓA

Mai Đình Hiếu