TÀI LIỆU ĐẶC TẢ CHỨC NĂNG HỆ THỐNG VNCERT

Version 1.1

Publication Details

Change Record

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Purpose |
| 1.0 | Thursday, June 27th, 2018 | Lam Thanh Tung | Created document. |
|  |  |  |  |

Document Properties

|  |  |
| --- | --- |
| File location: | \*\*\* |
| File name: | Guide Document |
| Last updated: |  |

Document authorisation

|  |  |
| --- | --- |
|  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
|  |  |
| ( ) |  |
| / / |  |
| **Review by:** | **Review By:** |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |

1. **Yêu cầu chung hệ thống**

* Là chương trình cung cấp cổng thông tin điện tử và đăng ký thành viên.
* Là công cụ quản lý, điều phối, ứng cứu sự cố an toàn thông tin.

1. **Yêu cầu chức năng phần mềm:**

Hệ thống sẽ bao gồm một số chức năng chính có mục đích như sau:

* + - * Nhóm chức năng cổng thông tin điện tử
      * Nhóm chức năng điều phối ứng cứu sự cố
      * Báo cáo

Yêu cầu công nghệ sử dụng :

Để xây dựng và triển khai Công Thông Tin Điện Tử , cần rất nhiều công cụ từ hệ điều hành đến cơ sở dữ liệu, ngôn ngữ lập trình:

* Visual Studio, Sublime Text: Môi trường phát triển tích hợp (Integrated Development Environment; viết tắt: IDE), sử dụng để viết và chỉnh sửa mã nguồn.
* Mircosoft SQL Server: Hệ quản trị cơ sở dữ liệu.
* Ngôn ngữ lập trình C#, .NET Framwork, HTML, CSS, JQuery: là ngôn ngữ lập trình, xử lý trên máy chủ.
* Internet Information Service(IIS) Manager: một chương trình dành cho máy chủ đối thoại qua giao thức HTTP.
* Hệ điều hành: Windows

1. **Các nhóm chức năng**



1. **Cổng thông tin điện tử**
2. **Sơ đồ User case tổng thể**



1. **Module quản trị hệ thống**
   1. *Quản lý cổng thông tin và trang thông tin*
   2. *Quản trị Banner Footer*
   3. *Quản trị các mẫu hiển thị nội dung*
   4. *Quản trị ngôn ngữ*
   5. *Thiết lập và quản trị danh sách danh mục nội dung thông tin*
   6. *Thiết lập và quản trị các loại menu*
   7. *Quản lý cấu hình*
   8. *Cài đặt, gỡ bỏ các khối chức năng trong khi hệ thống đang hoạt đông*
   9. *Quy trình đăng, kiểm duyệt và xuất bản thông tin*
   10. *Quản lý Backup & Restore*

* Cho phép xem danh sách Backup.
* Thêm mới các bản Backup.
* Restore: cho phép chọn bản Backup để restore.
  1. *Thống kê báo cáo*
* Cho phép thống kê tin bài: Theo chuyên mục tin; Theo người biên tập.
* Thống kê hỏi đáp: Theo trạng thái hỏi; Theo thời gian gửi câu hỏi;
* Theo chuyên mục; Theo thời gian trả lời; Theo người trả lời.

1. **Module quản trị người dùng**
   1. *Quản trị phân quyền người dùng*

* Là chức năng cho phép quản trị viên tạo lập và quản lý các phân quyền người dùng.
* Cho phép thêm, sửa xóa phân quyền
  1. *Quản trị người dùng*
* Là chức năng cho phép người quản trị tạo người dùng.
* Người quản trị có thể tạo ra các loại người dùng với chức năng khác nhau: quản trị viên, nhân viên, trưởng phòng, giám đốc.
* Thêm, sửa, xóa, di chyển người dùng.
  1. *Quản trị nhóm người dùng*
* Là chức năng cho phép người quản trị tạo loại người dùng.
* Phân quyền cho loại người dùng: chọn quyền cho loại người dùng trong danh sách các quyền.
* Thêm, sửa, xóa loại người dùng.

1. **Module Quản trị nội dung, tin tức**
   1. *Sơ đồ User case quản lý tin tức*



* 1. *Quản trị danh mục tin tức*
* Là chức năng cho phép tạo và quản lý các danh mục tin tức theo dạng cây.
  + Các danh mục có thể chứa danh mục con
* Thêm sửa xóa các danh mục.
* Di chuyển các danh mục.
* Ẩn hiện các danh mục.
* Danh mục tin tức được quản lý theo nhóm người dùng. Người dùng thuộc nhóm nào chỉ nhìn thấy các danh mục tin tức thuộc nhóm đấy.
  1. *Quản lý bài viết*
* Là chức năng cho phép viết bài theo các danh mục tin tức.
* Quy trình tạo bài viết:



* Mô tả:

1. Người dùng cấp nhân viên đăng nhập và vào phần quản lý bài viết tạo các bài viết và lưu lại. Bài viết sau khi được tạo ở trạng thái chờ duyệt, nhân viên có thể vào chỉnh sửa bài viết của mình
2. Người dùng cấp trưởng phòng vào phần quản lý bài viết có thể nhìn thấy và review các bài viết được nhân viên tạo, chỉnh sửa nếu cần thiết và duyệt lần 1. Bài viết sau khi được trưởng phòng duyệt sẽ có trạng thái đã sơ duyệt và sẽ không thể chỉnh sửa.
3. Người dùng giám đốc vào phần quản lý bài viết và nhìn thấy danh sách bài viết đã được người dùng cấp trưởng phòng duyệt lần 1 và tiến hành duyệt lần cuối. Trong trường hợp người dùng giám đốc không duyệt bài viết, bài viết sẽ chuyển sang trạng thái không duyệt và người dùng nhân viên có thể vào chỉnh sửa bài viết.
4. Sau khi được người dùng cấp giám đốc duyệt, hệ thống sẽ đăng bài viết vào danh mục tin tức tương ứng.
   1. *Quản lý bình luận, ý kiến bài viết*

* Cho phép quản tri viên xem danh sách bình luận của 1 tin bài.
* Xem chi tiết một bình luận.
* Tìm kiếm, xóa, duyệt, hủy duyệt bình luận.
  1. *Quản lý thu thập tin tức*
* Cho phép quản trị viên quản lý danh sách tên miền.
* Quản lý dữ liệu xóa bỏ.
* Quản lý cụm từ thay thế.
* Quản lý dữ liệu thu thập.

1. **Module Thủ tục hành chính**
   1. *Quản trị cơ quan ban hành*

* Xem danh sách cơ quan ban hành.
* Thêm, sửa, xóa các cơ quan ban hành.
* Ẩn / hiện và sắp xếp theo thứ tự.
  1. *Quản trị danh mục thủ tục*
* Xem danh sách danh mục thủ tục.
* Thêm, sửa, xóa các danh mục thủ tục.
* Ẩn / hiện và sắp xếp theo thứ tự.
  1. *Quản trị lĩnh vực*
* Xem danh sách danh mục thủ tục.
* Thêm, sửa, xóa các danh mục thủ tục.
* Ẩn / hiện và sắp xếp theo thứ tự.
  1. *Quản trị thủ tục hành chính*
* Xem danh sách thủ tục hành chính.
* Thêm, sửa, xóa, duyệt các thủ tục hành chính.
* Ẩn / hiện và sắp xếp theo thứ tự.
* Thêm file đính kèm- Xóa file đính kèm.
  1. *Thống kê báo cáo thủ tục*
* Cho phép quản trị viên theo thời gian, theo cơ quan ban hành, theo trạng thái.
* Xuất báo cáo dạng Excel.
  1. *Tìm kiếm tra cứu thủ tục hành chính*
* Cho phép tìm kiếm tra cứu theo thời gian, theo cơ quan ban hành, theo cấp ban hành, theo tiêu đề, theo nội dung
* Hiển thị kế quả tìm kiếm
* Sắp xếp kết quả theo thứ tự.

1. **Module Quản lý hỏi đáp, giao lưu & Thăm dò ý kiến**
   1. *Quản lý danh mục hỏi đáp*

* Thêm, sửa xóa danh mục.
  1. *Quản lý câu hỏi*
* Thêm sửa xóa câu hỏi.
* Tìm kiếm câu hỏi.
* Xem chi tiết câu hỏi.
* Trả lời câu hỏi.
* Kiểm duyệt câu hỏi.
  1. *Quản lý câu trả lời*
* Thêm sửa xóa câu trả lời.
* Tìm kiếm câu trả lời.
* Xem chi tiết câu trả lời.
* Kiểm duyệt câu trả lời.

1. **Module Quản lý Hình ảnh – vide**
   1. *Quản lý danh mục hình ảnh*

* Thêm sửa xóa danh mục.
* Tìm kiếm sắp xếp danh mục.
* Xem chi tiết danh mục.
* Duyệt / hủy duyệt danh mục
  1. *Quản lý Album ảnh*
* Thêm sửa xóa Album ảnh.
* Tìm kiếm sắp xếp Album ảnh.
* Xem chi tiết Album ảnh.
* Duyệt / hủy duyệt Album ảnh.
  1. *Quản lý danh mục video*
* Thêm sửa xóa danh mục video.
* Tìm kiếm sắp xếp danh mục video.
* Xem chi tiết danh mục video.
* Duyệt / hủy duyệt danh mục video.
  1. *Quản lý Album video*
* Thêm sửa xóa album video.
* Tìm kiếm sắp xếp album video.
* Xem chi tiết album video.
* Duyệt / hủy duyệt album video.
  1. *Quản lý video*
* Thêm sửa xóa video.
* Tìm kiếm sắp xếp video.

1. **Module Quản lý văn bản**
   1. *Quản trị cơ quan ban hành*

* Xem danh sách cơ quan ban hành.
* Thêm, sửa, xóa, duyệt các cơ quan ban hành.
* Ẩn / hiện và sắp xếp theo thứ tự.
  1. *Quản trị danh mục văn bản*
* Xem danh sách danh mục văn bản.
* Thêm, sửa, xóa, duyệt các danh mục văn bản.
* Ẩn / hiện và sắp xếp theo thứ tự.
  1. *Quản trị lĩnh vực*
* Xem danh sách lĩnh vực.
* Thêm, sửa, xóa, duyệt các lĩnh vực.
* Ẩn / hiện và sắp xếp theo thứ tự.
  1. *Quản trị văn bản*
* Xem danh sách văn bản.
* Thêm, sửa, xóa, duyệt các văn bản.
* Ẩn / hiện và sắp xếp theo thứ tự.
  1. *Tìm kiếm tra cứu văn bản*
* Cho phép tìm kiếm tra cứu theo thời gian, theo cơ quan ban hành, theo cấp ban hành, theo tiêu đề, theo nội dung
* Hiển thị kế quả tìm kiếm
* Sắp xếp kết quả theo thứ tự.

1. **Module Quản lý RSS**
   1. *Chuyên mục RSS*

* Thêm sửa xóa chuyên mục.
* Tìm kiếm sắp xếp chuyên mục.
* Xem chi tiết chuyên mục.
* Duyệt / hủy duyệt chuyên mục.
  1. *Quản lý danh sách kênh RSS*
* Thêm sửa xóa danh sách kênh.
* Tìm kiếm sắp xếp danh sách kênh.
* Xem chi tiết danh sách kênh.
* Duyệt / hủy duyệt danh sách kênh.

1. **Module Quản lý Menu và sitemap**
   1. *Quản lý sitemap*

* Thêm, sửa, xóa, các nhánh.
* Ẩn / hiện và sắp xếp theo thứ tự.

1. **Module Quản lý liên kết và quảng cáo**
   1. *Quản lý liên kết*

* Xem danh sách liên kết.
* Thêm, sửa, xóa, duyệt các liên kết.
* Ẩn / hiện và sắp xếp theo thứ tự.
  1. *Quản lý danh mục quảng cáo*
* Xem danh sách liên kết.
* Thêm, sửa, xóa, duyệt các liên kết.
* Ẩn / hiện và sắp xếp theo thứ tự.
  1. *Thông tin quảng cáo*
* Xem danh sách liên kết.
* Thêm, sửa, xóa, duyệt các liên kết.
* Ẩn / hiện và sắp xếp theo thứ tự.

1. **Module ứng dụng tra cứu thông tin**
   1. *Tìm kiếm thông tin*

* Tìm kiếm thông tin đã được báo cáo theo các tiêu chí:
  + Loại sự cố.
  + Mức độ sự cố .
  + Các vấn đề nóng đang gặp phải.
  + Báo cáo thống kê được phép công bố

1. **Quản lý thành viên mạng lưới**
2. **Sơ đồ Use case**



1. **Đăng ký thành viên**

* *Quy trình đăng ký thành viên*



* *Sơ đồ luồng dữ liệu*



* Sau khi đăng ký tài khoản người dùng có thể đăng ký trở thành thành viên mạng lưới.
* Để đăng ký là thành viên mạng lưới cần thực hiện các bước sau:

*Bước 1: Người dùng muốn đăng ký đơn vị thành viên cần điền các thông tin đăng ký trên form đăng ký.*

Thông tin đăng ký thành viên mới bao gồm:

* Thông tin chung về thành viên
* Thông tin về đầu mối tiếp nhận thông báo
* Thông tin về đầu mối liên lạc của hệ thống
* Giới thiệu về hạt động của đơn vị
* Thông tin về các hệ thống thuộc phạm vi phụ trách của đơn vị
* Thông tin về nhân lực của đơn vị thành viên
* Đầu mối liên lạc của đơn vị: trong giờ làm việc, ngoài giờ làm việc, người có thẩm quyền, và các phương tiện liên lạc khác

Sau khi thực hiện đăng ký đơn vị thành viên, hệ thống sẽ trả lại thông báo tiếp nhận hồ sơ đăng ký qua email.

*Bước 2: Tải hồ sơ đăng ký và phê duyệt đăng ký.*

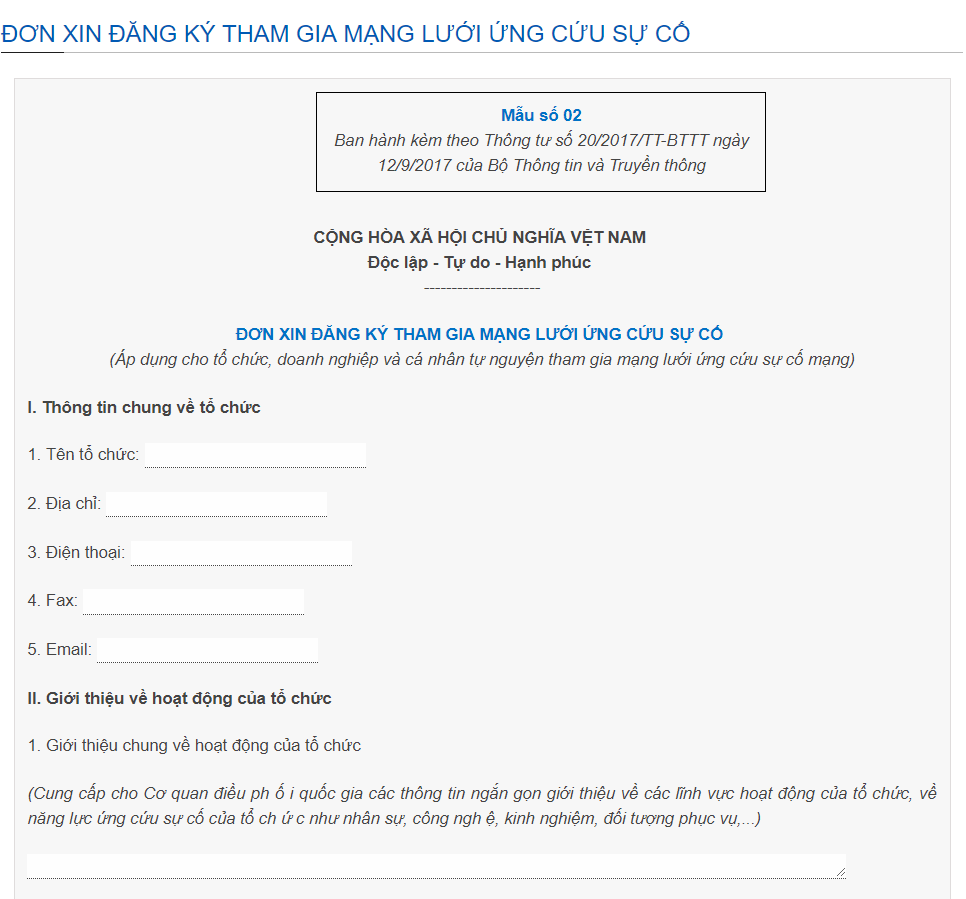
Người dùng quản trị có thể xem danh sách các đơn vị thành viên đang đăng ký, lọc sắp xếp theo thời gian.

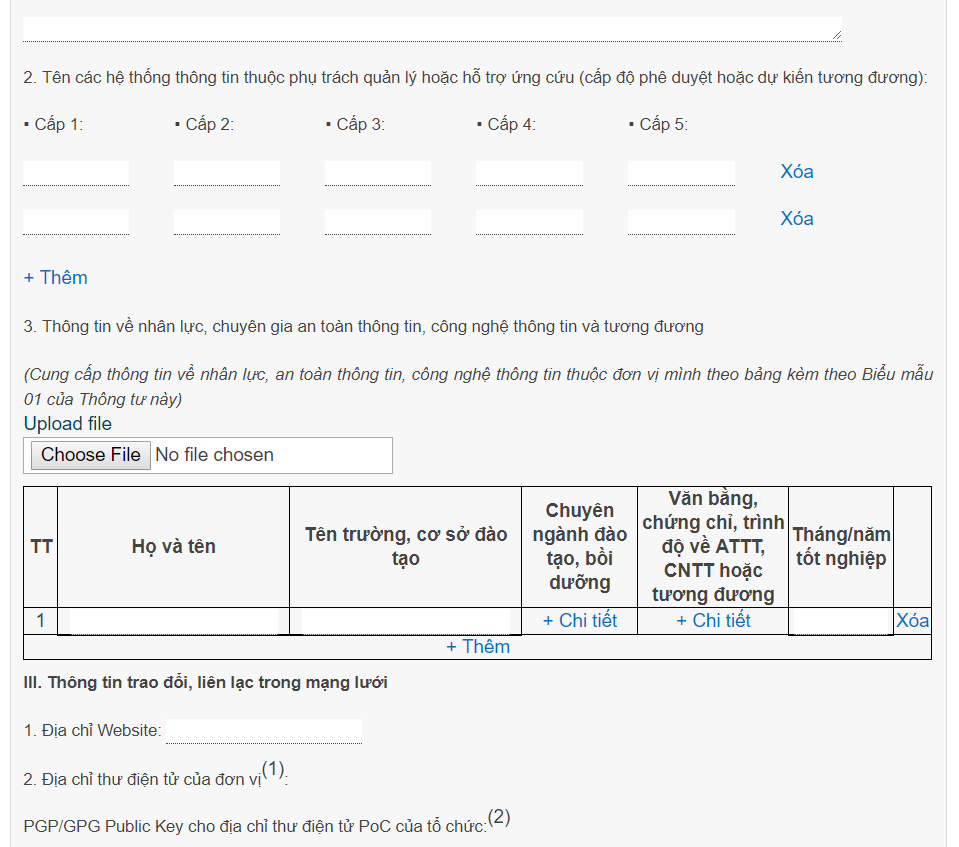
Khi được phê duyệt làm thành viên: người quản trị cần upload các file scan hồ sơ bản cứng của đơn vị thành viên lên hệ thống. Bấm nút phê duyệt đăng ký để hoàn thành.

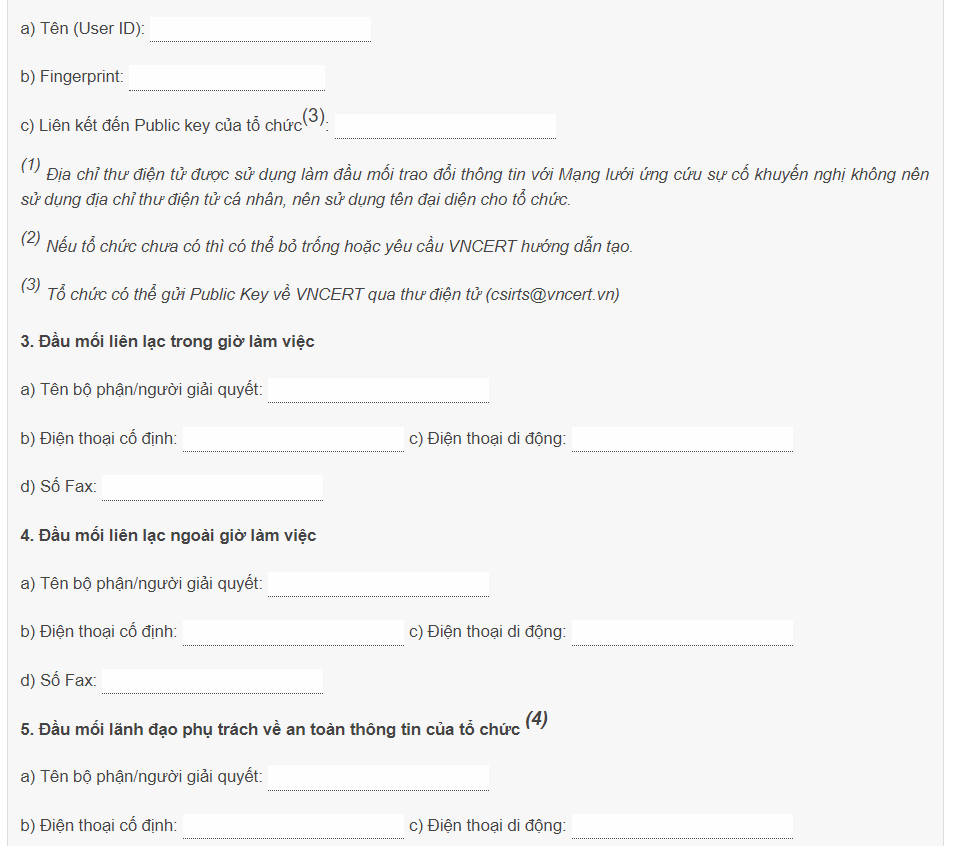
*Bước 3: Hệ thống gửi thông báo xác nhận hồ sơ đăng ký đơn vị thành viên đã được phê duyệt*

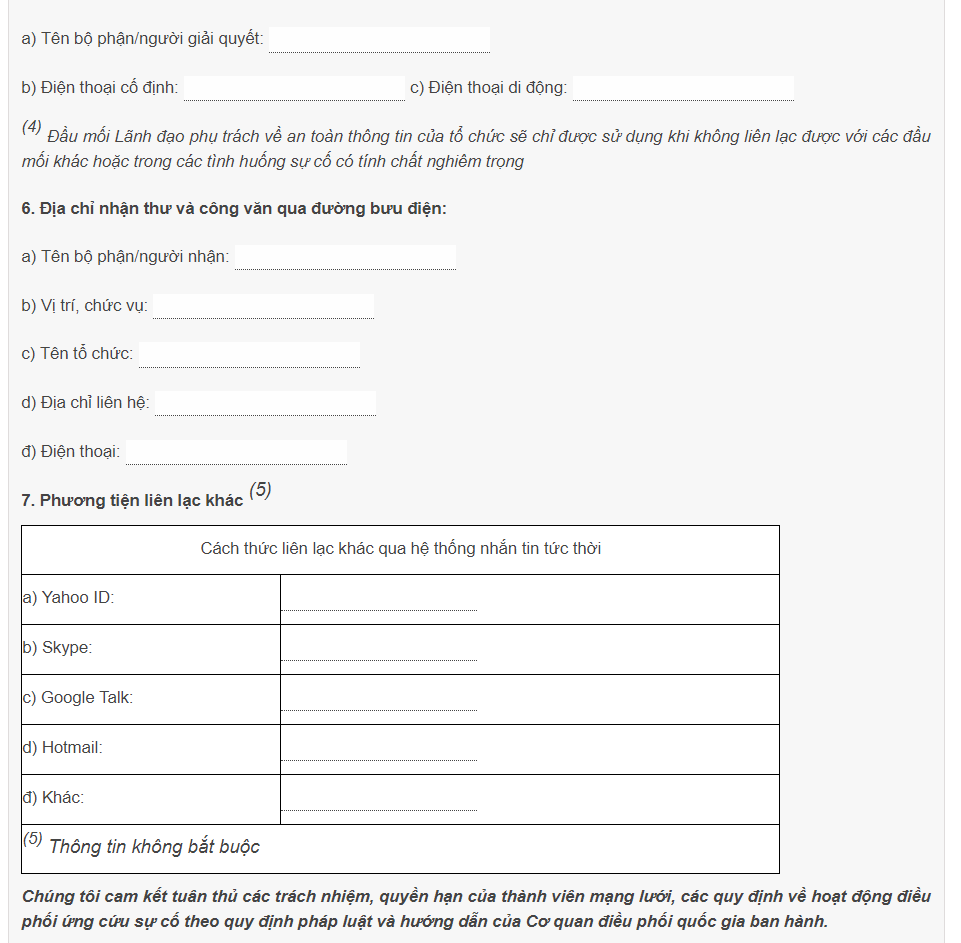
1. **Quản lý danh sách thành viên**

* Cho phép quản trị viên xem danh sách thành viên mạng lưới, xem thông tin chi tiết của thành viên.
* Thêm, sửa, xóa thành viên:
  + - Cho phép quản trị viên thêm thành viên theo văn bản đã được xác thực
    - Cho phép thành viên mạng lưới tạo các thành viên con trực thuộc. Các thành viên con phải được phê duyệt bởi quản trị viên hệ thống.
    - Đăng ký danh sách nhân sự điều phối sự cố
    - Đăng ký danh sách thông tin hệ thống thông tin của đơn vị thành viên
* Tìm kiếm thành viên theo các tiêu chí:
  + - Tên đơn vị
    - Loại đơn vị
    - Địa bàn hoạt động của đơn vị
    - Thời gian đăng ký thành viên
    - Trạng thái đơn vị thành viên
* Dừng và khôi phục tư cách thàn viên:
  + - Để thực hiện dừng đơn vị thành viên người quản trị cần upload bản scan các tài liệu liên quan đến việc dừng tư cách đơn vị thành viên.
    - Hệ thống sẽ thông báo đến đơn vị thành viên bằng email/tin nhắn về kết quả của việc dừng tư cách đơn vị thành viên
    - Để thực hiện khôi phục tư cách đơn vị thành viên, người quản trị cần tìm theo trạng thái “Đã dừng tư cách đơn vị thành viên” và upload bản scan các tài liệu liên quan đến việc khôi phục tư cách đơn vị thành viên.
    - Hệ thống sẽ thông báo đến đơn vị thành viên bằng email/tin nhắn về kết quả của việc dừng tư cách đơn vị thành viên.
* Biểu mẫu đăng ký thành viên









1. **Thành viên thông báo sự cố**

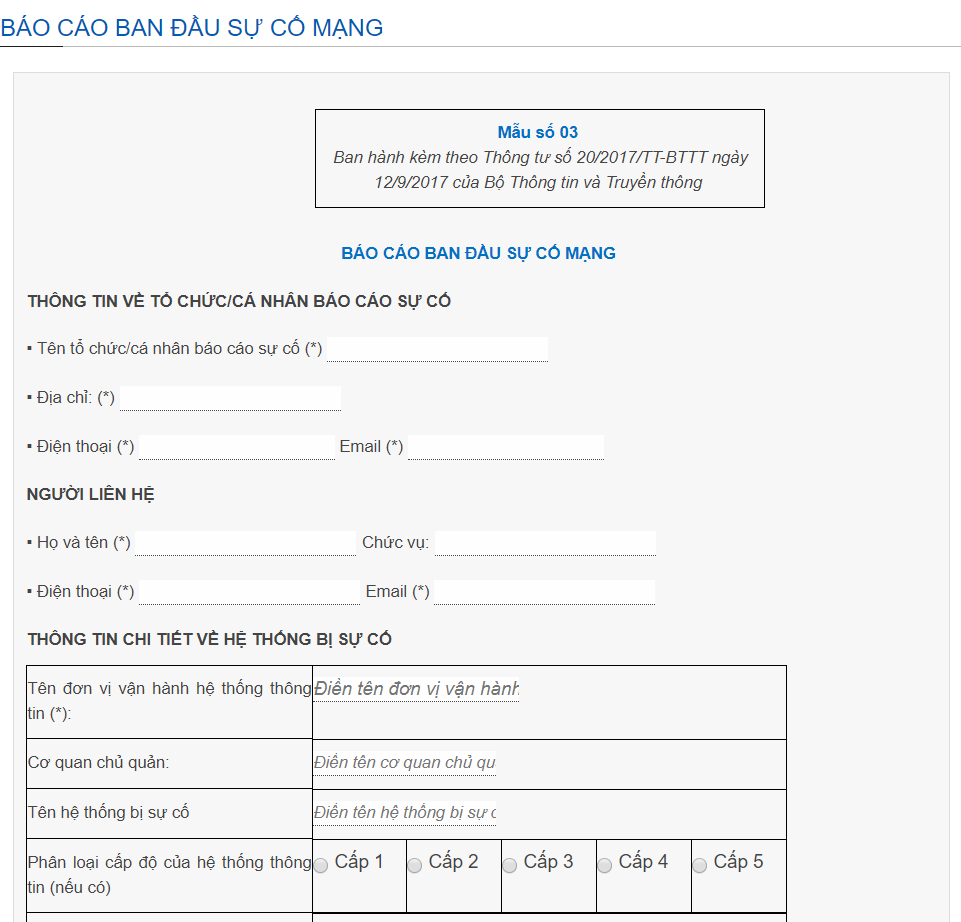
* *Quy trình thông báo sự cố*

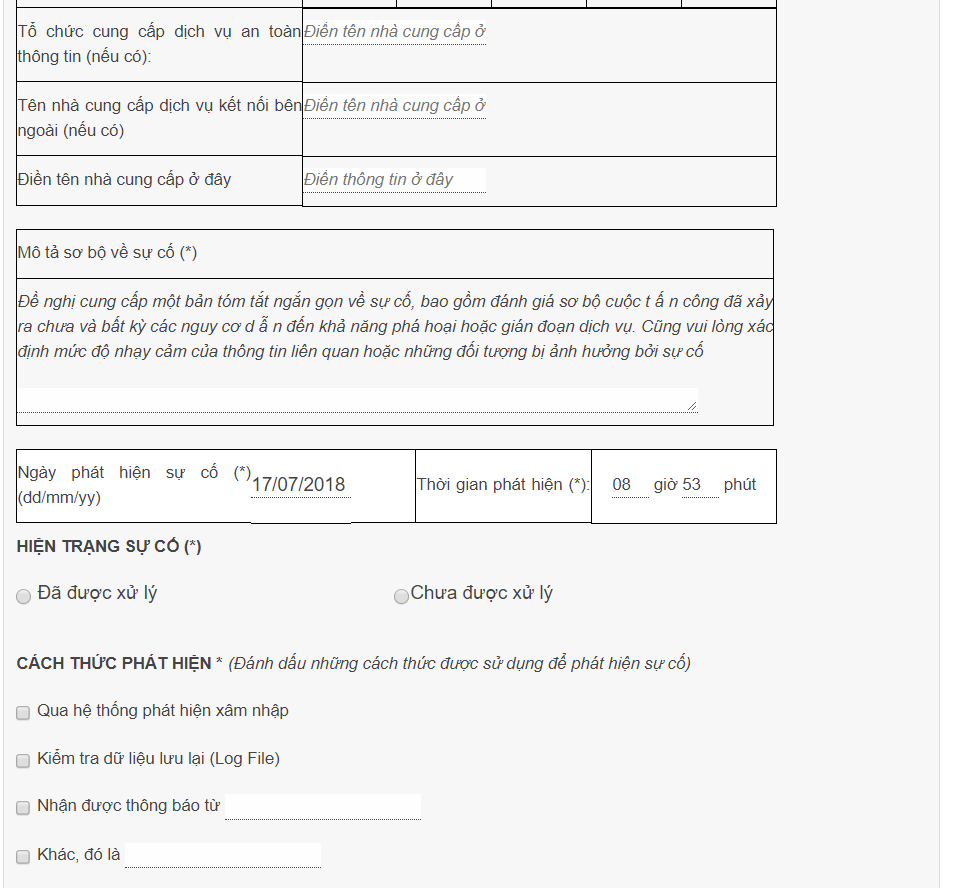


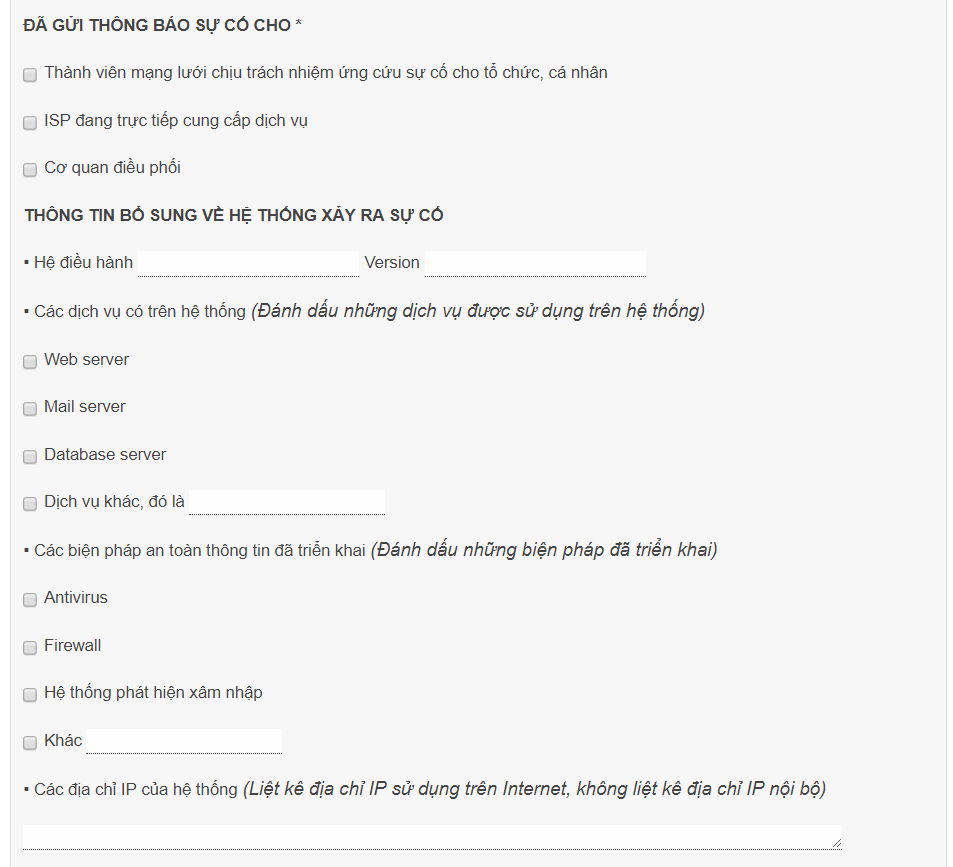
* *Sơ đồ luồng dữ liệu*

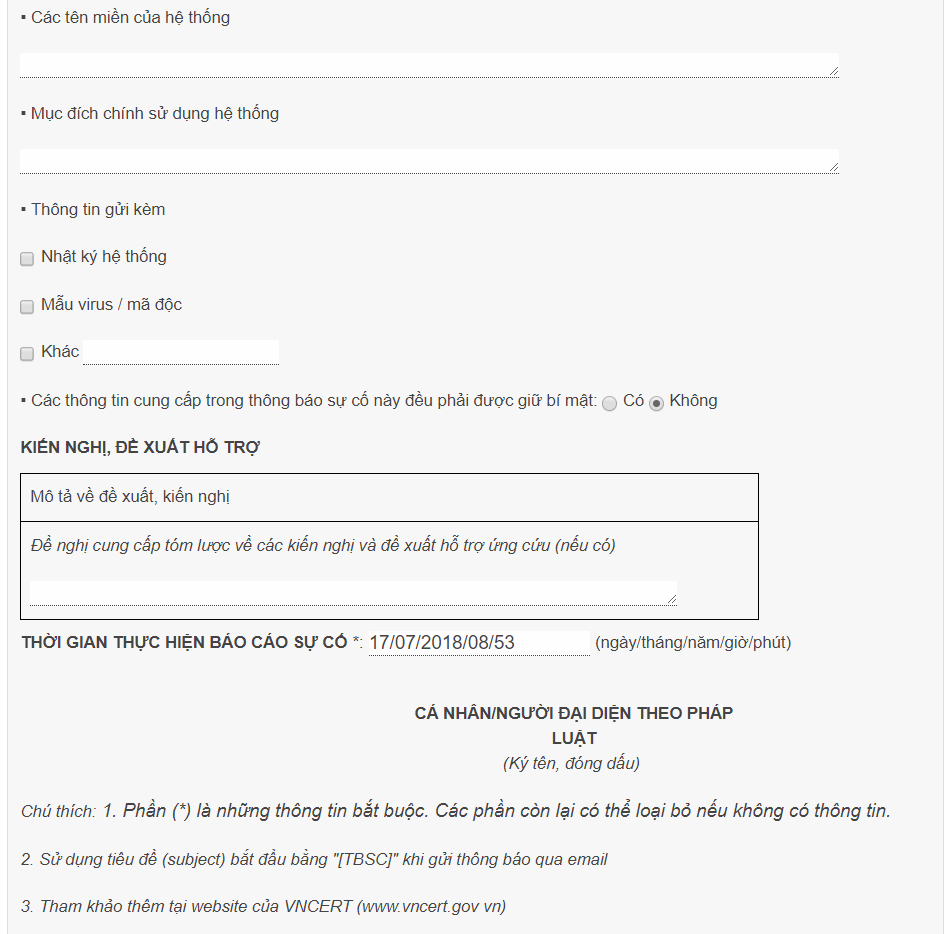


* + - Là chức năng cho phép các đơn vị thành viên, hoặc các đơn vị không phải là thành viên thông báo cho VNCert về các sự cố đang diễn ra tại đơn vị của mình.
    - Đơn vị thành viên thực hiện khai báo các vấn đề gồm các thông tin sau vào form thông báo:
    - Thông tin chung về đơn vị - lấy trong CSDL cho phép sửa thông tin đầu mối liên hệ:
    - Thông tin về hệ thống gặp vấn đề.
    - Lựa chọn các cấp độ phân loại vấn đề qua ma trận.
    - Mô tả về vấn đề
    - Ngày phát hiện vấn đề
    - Trạng thái của vấn đề: đã xử lý – chưa xử lý.
    - Cách thức phát hiện vấn đề.
    - Các đơn vị đã gửi thông báo
    - Các thông tin bổ sung về vấn đề
    - Kiến nghị đề xuất hỗ trợ.
    - Loại vấn đề (nếu loại vấn đề này được tồn tại trên hệ thống)
* Đơn vị thành viên thực cũng có thể gọi điện tới quản trị viên VNCert để thực hiện việc thông báo.
* Sau khi gửi báo cáo vấn đề phần mềm gửi thông báo tiếp nhận vấn đề qua email/tin nhắn đến đơn vị thành viên.
* Hệ thống cho phép quản trị viên kiểm tra thông cáo về sự cố xảy ra tại đơn vị, để đưa ra quyết định đóng sự cố hoặc điều phối nhân sự ứng cứu sự cố.
* Biểu mẫu thông báo sự cố

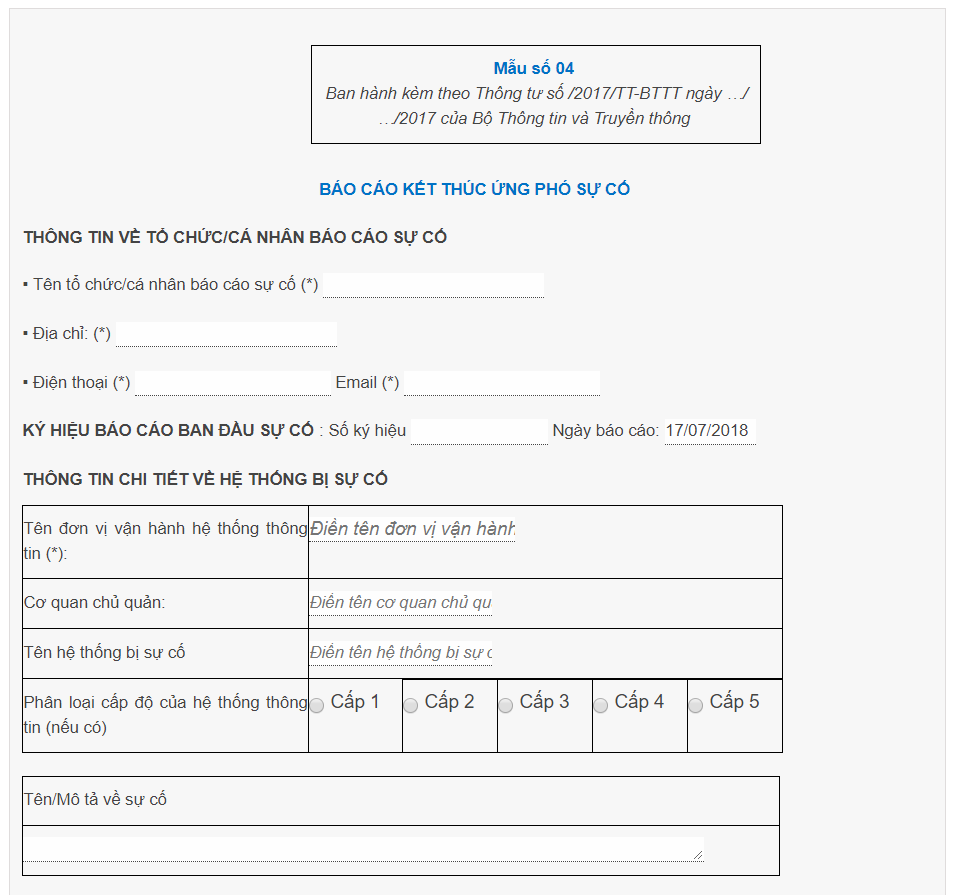


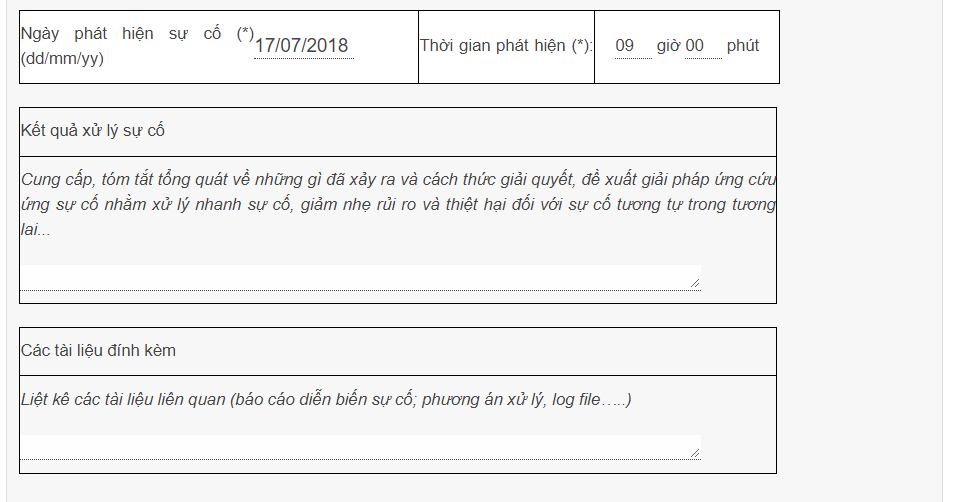
****

****

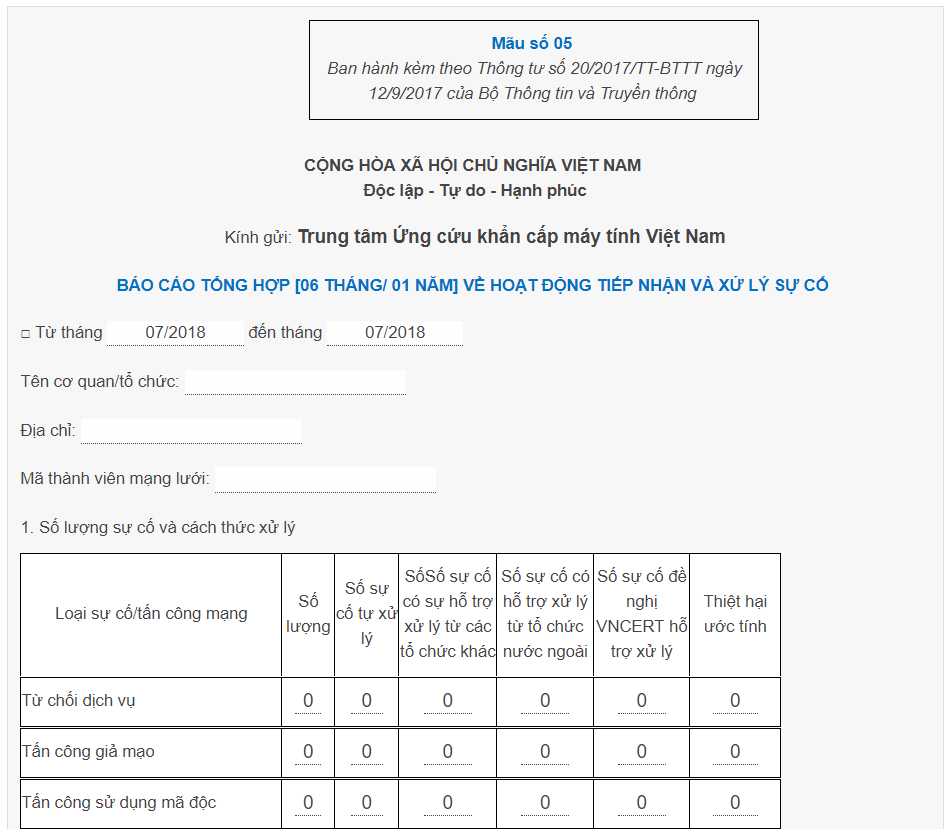
****

* Biểu mẫu thông báo kết thúc sự cố

****

****

* Biểu mẫu báo cáo tổng hợp sự cố



****

1. **Chức năng điều phối ứng cứu sự cố**

* ***Sơ đồ User case***



* ***Quy trình điều phối ứng cứu sự cố***



* ***Sơ đồ luồng dữ liệu***



**Quản lý sự cố**

* 1. ***Quản lý Attack***
     + Mô tả: Cho phép người quản trị quản lý các Attack nói chung. Các attack bao gồm tất cả các sự cố an toàn thông tin không thuộc các phần sự cố còn lại
     + Thông tin attack được gửi cho các thành viên đưa vào mục Dịch vụ cảnh báo (mục 4.2).
     + Thông tin Attack:

|  |
| --- |
| timestamp |
| IP |
| asn |
| geo |
| url |
| type (downadup) |
| http\_agent(Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)) |
| src\_port(1938,1499 ...) |
| hostname (static.vnpt.vn, localhost ) |
| dst\_port (Địa chỉ cổng đích) |
| protocol (udp or tcp) |
| servername |
| server |
| header (HTTP/1.1 200 OK) |
| tag (netis\_vulnerability,cwmp,memcached,rdp ...) |
| handshake |

* 1. ***Quản lý sự cố C&C botnet***
     + Mô tả: Cho phép người quản trị quản lý các sự cố C&C botnet.
     + Thông tin botnet.

|  |
| --- |
| timestamp |
| ip |
| asn |
| geo |
| url |
| type (downadup) |
| http\_agent(Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)) |
| src\_port(1938,1499 ...) |
| hostname (static.vnpt.vn, localhost ) |
| dst\_port (Địa chỉ cổng đích) |
| protocol (udp or tcp) |
| servername |
| server |
| header (HTTP/1.1 200 OK) |
| tag (netis\_vulnerability,cwmp,memcached,rdp ...) |

* 1. ***Quản lý sự cố Phishing***

Mô tả: Cho phép người quản trị quản lý các sự cố Phishing và gửi emai thông báo đến các đơn vị gặp sự cố.

* + - Hiển thị danh sách các sự cố.
      * Với các sự cố đến từ cùng một domain và xảy ra ở nhiều đường dẫn khác nhau, hệ thống sẽ hiển thị các đường dẫn này trong cùng một sự cố. Khi click vào những sự cố này sẽ hiện ra các link chi tiết.

Ví dụ:

http[:]//year2000vn.com[.]vn/resource/.www.paypaI.co.uk/signin/country=login/locale=ln\_ln/

http[:]//year2000vn.com[.]vn/resource/.www.paypaI.co.uk/signin/country=login/locale=ln\_ln/rev.php

* + - Import các sự cố từ file excel.
      * Hệ thống đọc file excel và sử dụng API để lấy thông tin về IP, ISP của sự cố.
      * Link API: <https://whois.domaintools.com>.
    - Sửa, xóa các sự cố.
    - Gửi email đến đơn vị gặp sự cố.
      * Hệ thống cho phép quản trị viên tạo email theo mẫu có sẵn và gửi cho các đơn vị gặp sự cố.
      * Hệ thống tự động lấy email nhận từ thông tin của các thành viên của hệ thống, nếu đơn vị chưa là thành viên hoặc chưa có email, người quản trị sẽ điền thông tin này.
      * Cho phép sửa nội dung mẫu email.
      * Nội dung mẫu Email (xem mục 5.3).
    - Kiểm tra và đóng sự cố.
      * Người quản trị nhận email trả lời của đơn vị gặp sự cố trong mục Hỗ trợ xử lý, người quản trị có thể xem và trả lời email ở đây.
      * Người quản trị kiểm tra nếu sự cố đã được xử lý thì đóng sự cố. Khi đó, trạng thái của sự cố sẽ chuyển từ “Còn tồn tại” thành “Đóng”.
    - Thông tin Phishing

|  |
| --- |
| Link phishing |
| Đích giả mạo |
| Nguồn Thông tin |
| Thời gian |
| IP |
| Thông tin ISP |

* 1. ***Quản lý sự cố Deface*** 
     + Tương tự mục (2.3)
     + Thông tin Deface

|  |
| --- |
| Link Deface |
| Thời gian |
| Nguồn Thông tin |
| Nguười tấn công |
| IP |
| Thông tin ISP |

* 1. ***Quản lý sự cố Malware***
     + Tương tự mục (2.3)

|  |
| --- |
| Link nhiễm malware |
| Tên virus |
| IP |
| IPS |
| Thời gian |
| Nguồn Thông tin |

* + - Hệ thống tự động kiểm tra các sự cố malware xem còn tồn tại không và thực hiện việc đóng sự cố nếu như đã được giải quyết.

1. **Quản lý mẫu email**

Là chức năng cho phép quản trị viên chỉnh sửa nội dung mẫu email thông báo sự cố đến các thành viên.

Nội dung mẫu email:

**Email tiếp nhận:** Lấy từ danh sách mục ISP (có thể sửa được)

**Email CC:** là email để báo cáo (mặc định: [tnchung@vncert.vn](mailto:tnchung@vncert.vn)) hoặc thêm sửa.

**Tiêu đề:** *Đề nghị xử lý sự cố trên dịch vụ của (Tên đơn vị ISP,)*

**Nội dung:**

*Kính gửi (Tên đơn vị ISP)*

*Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam, Bộ Thông tin và Truyền thông (VNCERT) ghi nhận, hiện có những domain*

*(Các hoặc một domain bị sự cố vidu nếu click vào email ở đầu đường link*

*http[:]//year2000vn.com[.]vn*

*trong nội hiển thị:*

*http[:]//year2000vn.com[.]vn/resource/.www.paypaI.co.uk/signin/country=login/locale=ln\_ln/*

*http[:]//year2000vn.com[.]vn/resource/.www.paypaI.co.uk/signin/country=login/locale=ln\_ln/rev.php*

*)*

*(IP bị sự cố)*

*IP này  thuộc (Tên đơn vị ISP,)  
  
Thực hiện Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ và Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc, Trung tâm VNCERT đề nghị Quý Công ty xử lý sự cố (giả mạo (phishing), nhiễm mã độc (malware), (thay đổi giao diện) Deface ), và các cố (giả mạo (phishing), nhiễm mã độc (malware), (thay đổi giao diện) Deface ) trong vòng 24 giờ kể từ khi nhận được Email này nhằm ngăn chặn website cố (giả mạo (phishing), nhiễm mã độc (malware), (thay đổi giao diện) Deface ).  
  
Sau khi hoàn thành việc xóa các website cố (giả mạo (phishing), nhiễm mã độc (malware), (thay đổi giao diện) Deface ), đề nghị Công ty gửi báo cáo kết thúc sự cố (ban hành kèm theo Thông tư số 20/2017/TT-BTTTT, có thể tải tại địa chỉ:*[*http://vncert.vn*](http://vncert.vn/)*) về Đầu mối tiếp nhận sự cố của Trung tâm VNCERT qua địa chỉ*[*ir@vncert.vn*](mailto:ir@vncert.vn) *Cảm ơn sự hợp tác của Quý Công ty.*

*--------------------------------------------  
Nguyen Thanh Chuong (Mr)  
VNCERT, MIC  
Mobile:*[*+84 91 8228 754*](callto:+84%2091%208228%20754)*Website:*[*www.vncert.gov.vn*](http://www.vncert.gov.vn/)

1. **Dịch vụ cảnh báo**

* *Quy trình sử dụng dịch vụ cảnh báo*



* Hệ thống cho phép các đơn vị thành viên đăng ký nhận email cảnh báo mỗi khi có sự cố xảy ra với các domain do đơn vị quản lý.
* Đơn vị thành viên đăng ký các dải IP(domain) nhận cảnh báo, hệ thông so sánh giải ip với các ip thuộc sự cố (trong mục attack, malware, phishing,deface) thông kê nếu có ip trùng thì báo cáo sự cố theo mẫu dưới và kèm theo file đính kèm thông báo chi tiết sự cố:

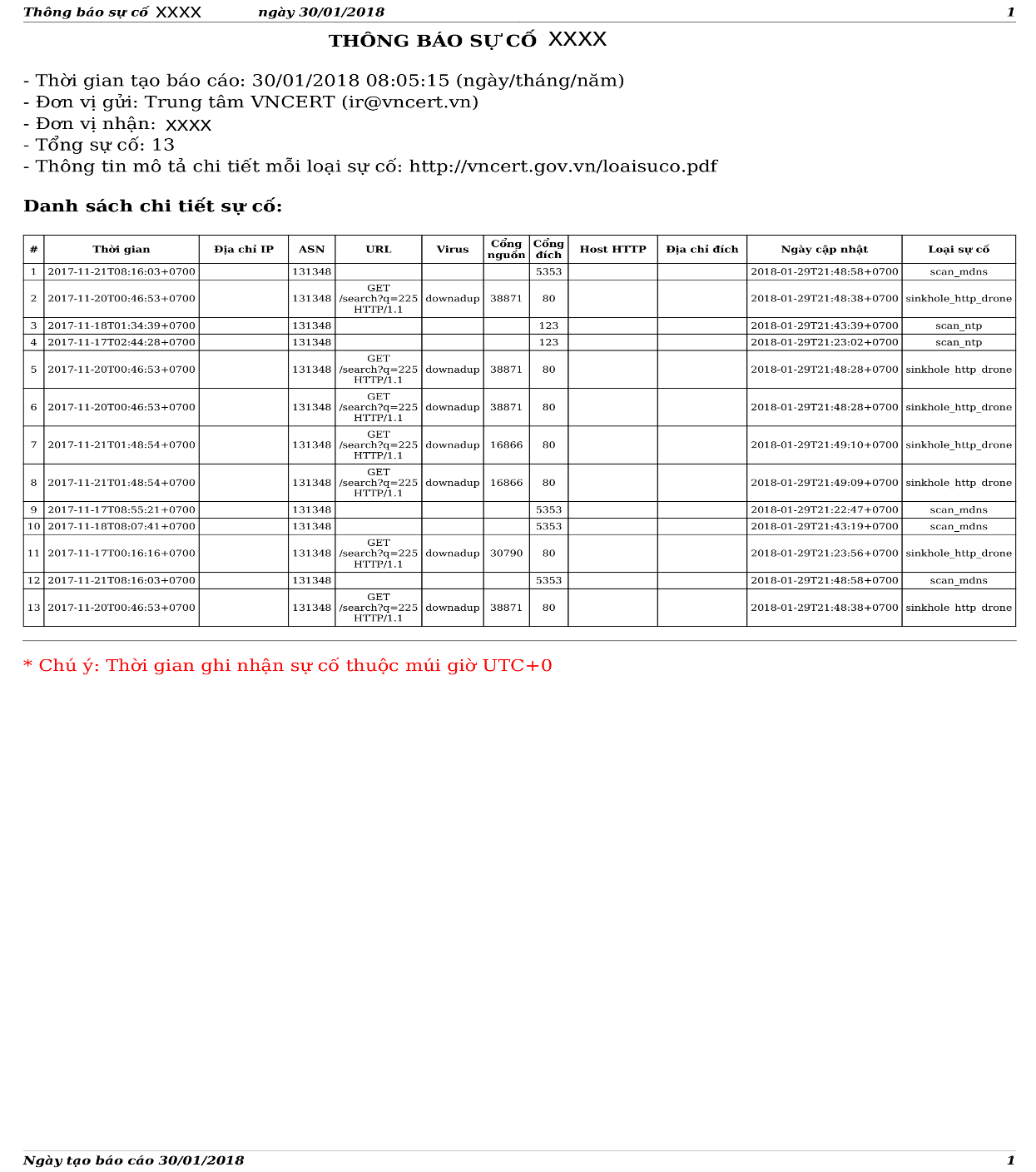
*Kính gửi đầu mối tiếp nhận sự cố XXX,*

*Trong quá trình theo dõi sự cố tại Việt Nam, Trung tâm VNCERT phát hiện các sự cố liên quan đến XXXX.*

*Danh sách các sự cố được gửi trong tập tin đính kèm (nếu có, nếu không có sẽ không có file đính kèm).*

*Trân trọng./.*

* + - File đính kèm có dạng yyyymmdd\_XXX\_Report.pdf
    - Thành viên có thể cài đặt thời gian nhận cảnh báo vào một giờ nhất định trong ngày theo giờ GMT+7.
    - Nhận báo cáo theo ngày, tuần, tháng, quý, năm.
    - Mẫu báo cáo được tạo từ template có sẵn và có thể sửa lại các template.



1. **Quản lý CVE**

Là chức năng cho phép người quản trị quản lý các bản cập nhật, bản vá lỗi mới nhất của các hệ thông thông tin của các đơn vị thành viên.

* + - Người quản trị import file chứa các CVE vào hệ thống.
    - Gửi email đến các đơn vị thành viên với các CVE phù hợp
      * Hệ thống tự động lọc các CEV theo các hệ thống thông tin của cá đơn vị thành viên đã đăng ký để gửi thông tin các bản vá lỗi, bản cập nhật phù hợp.
    - Thông tin CVE

|  |
| --- |
| CVE ID |
| Vulnerability Type(s) (Exec Code,DoS CSRF,+Info, XSS ...) |
| Product |
| Publish Date |
| Update Date |
| Score |
| Gained Access Level (None) |

1. **Quản lý tin nội bộ**

* Là chức năng cho phép quản trị viên tạo các tin tức và phân quyền cho các thành viên trong hệ thống vào xem.
* Tin tức bao gồm: các tin tức mới nhất về an toàn thông tin trong tuần và thống kê các sự cố, tổng hợp các lỗ hổng, bản vá bảo mật trên các sản phẩm/dịch vụ phổ biến tại Việt Nam.
* Tài khoản quản trị viên duyệt tin tức do người dùng tạo.
* Phân quyền cho các thành viên được xem những mục tin tức nào. Người quản trị có thể tùy biến các quyền xem cho từng thành viên.
* Danh sách các mục thông tin trong tin tức

Tình hình tấn công gây nguy hại trên các trang web tại Việt Nam.

Theo dõi, phân tích, phát hiện các dấu hiệu, nguy cơ ảnh hưởng đến tính sẵn sàng của Cổng/Trang thông tin điện tử cấp Bộ, tỉnh hoặc tương đương.

Lỗ hổng/điểm yếu an toàn thông tin trong tuần(CVE).

Hoạt động một số mạng botnet, APT, mã độc tại Việt Nam.

Theo dõi, thu thập, thống kê thông tin nổi bật về an toàn thông tin trong kỳ báo cáo: phishing, malware, deface.

1. **Báo cáo thống kê sự cố**

* Là chức năng cho phép xem các báo cáo về sự cố dựa theo thời gian(từ ngày đến ngày).
* Báo cáo theo từng thành viên.
* Check sự cố trùng: nếu có các sự cố trùng lặp từ 2 hoặc nhiều hơn trong khoảng thời gian trích xuất báo cáo thì chỉ thống kê là một sự cố.
* Các loại báo cáo:
  + - * + Phishing
      * Báo cáo Top Target Phishing: top các domain bị tấn công Phishing nhiều nhất trong khoảng thời gian được chọn.
      * Báo cáo TOP ISP: top các đơn vị ISP bị tấn công Phishing nhiều nhất trong khoảng thời gian được chọn.
        + Deface
      * Báo cáo TOP ISP: top các đơn vị ISP bị tấn công Deface nhiều nhất trong khoảng thời gian được chọn.
        + Malware
      * Báo cáo Top Virus name: top các tên virus xuất hiện nhiều nhất trong khoảng thời gian được chọn.
      * Báo cáo TOP ISP: top các đơn vị ISP bị Malware tấn công nhiều nhất trong khoảng thời gian được chọn.
        + Botnet
      * Báo cáo TOP ISP: top các đơn vị ISP bị tấn công nhiều nhất trong khoảng thời gian được chọn.
* Hệ thống cho phép xuất báo cáo theo ngày tháng dưới dạng excel và pdf.