**1. Mẫu đề án cung cấp dịch vụ mạng xã hội trực tuyến - Mẫu 01:**

**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**

**Độc lập - Tự do - Hạnh phúc**

**ĐỀ ÁN CUNG CẤP DỊCH VỤ MẠNG XÃ HỘI TRỰC TUYẾN**

**I. Các chuyên mục cung cấp cho người dùng của mạng xã hội trực tuyến trên website……**

Tên miền website chính là http://...... Đây là một website cung cấp các dịch vụ mạng xã hội trực tuyến với mục tiêu chính là kết nối những người (cá nhân, tổ chức) kinh doanh online. Trang web có một giao diện khá bắt mắt và có tính mỹ thuật cao. Về ngôn ngữ, nhằm mục đích kết nối những người kinh doanh online là người Việt Nam nên Website sử dụng hoàn toàn bằng tiếng Việt vì thế người dùng có thể chia sẻ, trao đổi kinh nghiệm với nhau một cách dễ dàng và thuận tiện nhất. Giao diện của web được xây dựng hoàn toàn theo tiêu chuẩn ....... với những chức năng chính như Trang chủ, chia sẻ kinh nghiệm, Hỏi - đáp, Hỗ trợ.

Các chuyên mục chính cung câp cho người dùng dự kiến của website đó chính là:

- Trang chủ: đây chính là kiến trúc tổng thể của website, tại đây sẽ giới thiệu những nội dung như: hoạt động của cộng đồng thành viên, các thông tin kinh doanh nổi bật, những bài viết mới,…

- Chia sẻ kinh nghiệm: về công việc, về kinh doanh,…

- Trò chuyện trực tuyến

- Cẩm nang kinh doanh online;

- Chia sẻ tư liệu;

- Tìm kiếm bạn bè.

**II. Các tính năng của website mang đến cho người dùng**

Tại website sẽ mang đến cho người dùng những tính năng:

- Viết bài, cung cấp các thông tin về tình hình kinh doanh trong và ngoài nước cho những thành viên khác:

+ Tại tính năng này thì các bài giảng, kiến thức, thông tin về kinh doanh online sẽ được chính các chuyên gia trong ngành hay các chủ doanh nghiệp là cộng tác viên của website biên soạn

- Thực hiện trao đổi, chia sẻ các thông tin với những thành viên khác về những kinh nghiệm kinh doanh online

- Chia sẻ các tài liệu liên quan đến kinh doanh, bán hàng trực tuyến;

- Trò chuyện giữa các thành viên trực tuyến;

- Tính năng tìm kiếm các bạn bè;

- Tính năng lập nhóm kinh doanh.

**III. Kiểm duyệt các thông tin được đăng trên Website:**

Tất cả các thông tin được đăng lên Website (kể cả bài giảng, kiến thức và các thông tin khác được chia sẻ bởi các thành viên) đều được Website kiểm duyêt kỹ càng nhằm đảm bảo tính xác thực, đảm bảo về nội dung sao cho phù hợp với quy định của pháp luật, không vi phạm về văn hóa và thuần phong mỹ tục của người Việt Nam.

Kiểm duyệt sẽ được thực hiện qua 2 hình thức đó chính là: Kiểm duyệt bằng đội ngũ nhân sự và qua hệ thống phần mềm tự động kiểm duyệt.

Những vấn đề cần kiểm duyệt bao gồm: nội dung, hình ảnh, âm thanh.

Các bước thực hiện kiểm duyệt như sau:

- Bước 1: Kiểm duyệt lần 1:

+ Thực hiện kiểm duyệt bằng hệ thống kỹ thuật đã triển khai các bộ lọc nội dung. Cụ thể là kiểm duyệt nội dung các thông tin qua bộ lọc từ khóa nhằm mục đích ngăn chặn những nội dung xấu. Danh sách từ khóa bị ngăn chặn sẽ được xây dựng dựa trên cơ sở các quy định của pháp luật. Ví dụ như các từ khoá mà có nội dung chống lại nhà nước; nội dung gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội; nội dung phá hoại khối đại đoàn kết toàn dân; nội dung tuyên truyền chiến tranh xâm lược; nội dung gây hận thù, gây mâu thuẫn giữa các dân tộc, sắc tộc, tôn giáo; nội dung tuyên truyền kích động; nội dung liên quan đến bạo lực, dâm ô, đồi trụy hoặc có liên quan đến tội ác, tệ nạn xã hội, mê tín dị đoan;…

+ Khi hệ thống phát hiện hoặc nghi ngờ có các nội dung vi phạm liên quan đến những  vấn đề này thì hệ thống sẽ tự động chuyển các nội dung vi phạm sang thành dạng cảnh báo và chờ xử lý.

- Bước 2: Kiểm duyệt lần 2: Thông qua đội ngũ nhân sự kiểm duyệt:

+ Bộ phận kiểm duyệt nội dung của doanh nghiệp sẽ phải trực tiếp kiểm tra lại các cảnh báo của hệ thống và sẽ đưa ra quyết định nên xóa bỏ hay là cho phép hiển thị các nội dung mà hệ thống cảnh báo.

+ Hằng ngày, bộ phận kiểm duyệt sẽ thực hiện việc kiểm duyệt các thông tin trong danh sách cảnh báo do hệ thống cập nhật và những nội dung vi phạm sẽ được xóa bỏ ngay lập tức.

+ Tùy vào mức độ vi phạm mà bạn quản trị Website sẽ xem xét quyết định thực hiện khóa tạm thời hoặc khóa vĩnh viễn tài khoản của những thành viên đăng tải các nội dung vi phạm.

+ Bộ phận kiểm duyệt còn thực hiện việc kiểm duyệt thông tin thông qua các thông báo về nội dung xấu của các thành viên khác. Khi bắt đầu nhận được thông báo thì bộ phận kiểm duyệt có nhiệm vụ xác nhận lại các thông tin này và nếu phát hiện có vi phạm thì sẽ xử lý theo quy trình chung.

**IV. Thông tin của công ty:**

Công ty.........có trụ sở tại...., được thành lập theo giấy chứng nhận đăng ký doanh nghiệp số......, do sở Kế hoạch và Đầu Tư....cấp ngày....

**V. Về chức năng, nhiệm vụ của nhân sự công ty:**

-  Đối với Giám đốc: sẽ chịu trách nhiệm chính, thực hiện hoạch định, phụ trách, và kiểm tra các thông tin xuất bản trên website và thực hiện xử lý các thông tin phản hồi từ bạn đọc cũng như từ cơ quan chức năng.

- Nhân viên thông tin: thực hiện tập hợp, xử lý thông tin và cập nhật thông tin.

- Nhân viên phát triển: phụ trách việc phát triển website về kỹ thuật, luôn đảm bảo website hoạt động ổn định và bảo mật.

**VI. Cơ sở hạ tầng của mạng xã hội website:**

Website có ưu điểm về cơ sở hạ tầng kỹ thuật hiện đại, có dung lượng kết nối internet lớn, sẽ đảm bảo được hệ website dùng để cung cấp mạng xã hội trực tuyến luôn trong trạng thái hoạt động ổn định. Công ty đã trang bị một loạt hệ thống máy tính có cấu hình cao và dùng hệ thống đường truyền tốc độ cao của nhà cung cấp dịch vụ xếp hàng đầu tại Việt Nam là..... Ngoài ra, chúng tôi cũng là một trong những công ty có thế mạnh về phát triển kinh doanh trên internet chính vì thế, chúng tôi khẳng định sẽ có đủ các phương tiện kỹ thuật và những đội ngũ nhân sự có trình độ đảm bảo mạng xã hội trực tuyến Website luôn trong tình trạng hoạt động tốt và ổn định. Do tầm quan trọng của hệ thống xây dựng đối với trang thông tin điện tử cung cấp mạng xã hội trực tuyến nên hệ thống cơ sở hạ tầng của website sẽ được thiết lập dựa trên những cơ sở sau:

- Sử dụng các công nghệ  mạng và sử dụng máy tính tiên tiến nhất hiện nay

- Tính ổn định: Hệ thống được thiết kế nhằm đảm bảo được khả năng hoạt động liên tục

- Độ tin cậy ( tính bảo mật của hệ thống): Đảm bảo được độ tin cậy với việc sử dụng các giao thức chuẩn tiên tiến nhất hiện nay

- An ninh mạng và thông tin trên mạng: áp dụng các giải pháp nhằm đảm bảo an toàn an ninh mạng bằng việc sử dụng giải pháp Firewall. Phối hợp với những cơ quan chức năng có thẩm quyền, áp dụng các quy định của pháp luật về việc cung cấp các thông tin trên Internet, các quy trình kiểm tra kiểm soát dịch vụ.

**Đại diện pháp luật của công ty Cổ phần Thanh Anh**

Họ và tên: Nguyễn Thị A

Chức vụ: Giám đốc công ty Cổ phần Thanh Anh

**2. Mẫu đề án cung cấp dịch vụ mạng xã hội trực tuyến - Mẫu 02:**

|  |  |
| --- | --- |
| **CÔNG TY** **……………………………** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM****Độc lập – Tự do – Hạnh phúc****Hà Nội, ngày … tháng … năm 20…** |

**ĐỀ ÁN  CUNG CẤP**

**DỊCH VỤ MẠNG XÃ HỘI TRỰC TUYẾN**

**I. Lời mở đầu**

Tài liệu Đề án thiết lập mạng xã hội trực tuyến này là của Công ty ............................................. xây dựng.

Tài liệu cung cấp thông tin về phương thức tổ chức mạng xã hội, các loại hình dịch vụ, phạm vi, lĩnh vực thông tin trao đổi và thông tin về địa điểm đặt hệ thống máy chủ tại Việt Nam, phương án tổ chức nhân sự, kỹ thuật, quản lý thông tin, tổ chức nhằm bảo đảm hoạt động của mạng xã hội.

Đồng thời đưa ra kiến nghị cấp giấy phép hoạt động mạng xã hội trực tuyến nhằm góp phần nâng cao khả năng ứng dụng tin học và tận dụng thành quả công nghệ thông tin để phục vụ cầu khai thác, chia sẻ, trao đổi thông tin, giao lưu kết bạn và học tập kiến thức về âm nhạc của người sử dụng Internet tại Việt Nam và trên thế giới.

**II. Giới thiệu chung về doanh nghiệp và mạng xã hội .................**

**2.1. Thông tin khái quát:**

a) Tên miền: .................

b) Tổ chức thiết lập website: Công ty .......................................................

Địa chỉ trụ sở chính:

Điện thoại:                               Emai:

c) Người chịu trách nhiệm chính:

Sinh năm:

Nơi đăng ký hộ khẩu thường trú:

CMND số:                     cấp tại                  ngày     tháng     năm

- Chức danh: Quản lý nội dung

- Số điện thoại liên lạc (cố định và di động):

Cố định :                                    Di động :

**2.2. Giới thiệu chung doanh nghiệp**

Công ty ...................................... được thành lập ngày 02/06/..... với các ngành nghề kinh doanh gồm :

|  |  |
| --- | --- |
| Mã ngành, nghề kinh doanh | Tên ngành, nghề kinh doanh |
| 1811 | In ấn |
| 1812 | Dịch vụ liên quan đến inChi tiết: - Đóng sách thành quyển, tạp chí, sách quảng cáo, catalo,…bằng cách gấp, xếp, khâu, dán hồ, kiểm tra thứ tự (trang sách), khâu lược, dán bìa, tỉa, xén, in tem vàng lên sách; - Xếp chữ, sắp chữ, sắp chữ in, nhập dữ liệu trước khi in bao gồm quét và nhận biết chữ cái quang học, tô màu điện tử; - Dịch vụ làm đĩa bao gồm sắp hình ảnh và sắp đĩa (để in ốp sét và in sắp chữ); - Khắc chạm, khắc axit trên trục lăn cho khắc kẽm; - Xử lý đĩa trực tiếp sang đĩa (cũng bao gồm đĩa nhựa); - Chuẩn bị đĩa và nhuộm nhằm làm giảm công việc in ấn và dán tem; - In thử; - Các sản phẩm nghệ thuật bao gồm in thạch bản và mộc bản (phiến gỗ để làm các bản khắc); - Sản xuất các sản phẩm sao chụp; - Thiết kế các sản phẩm in như bản phác thảo, maket, bản nháp; - Các hoạt động đồ họa khác như khắc rập khuôn, rập khuôn tem, in nổi, in dùi lỗ, chạm nổi, quét dầu và dát mỏng, kiểm tra thứ tự và sắp xếp. |
| 1820 | Sao chép bản ghi các loạiChi tiết: - Sao chép băng, đĩa hát, đĩa compact và băng máy từ các bản gốc; - Sao chép băng, đĩa từ, băng video phim và các ấn phẩm video từ các bản gốc; - Sao chép các phần mềm và dữ liệu sang đĩa, băng từ các bản gốc. |
| 6311 | Xử lý dữ liệu, cho thuê và các hoạt động liên quan |
| 6312 | Cổng thông tinChi tiết: : Hoạt động điều hành các website sử dụng công cụ tìm kiếm để tạo lập và duy trì các cơ sở dữ liệu lớn các địa chỉ internet và nội dung theo một định dạng có thể tìm kiếm một cách dễ dàng Hoạt động điều hành các website khác hoạt động như các cổng internet, như các trang báo chí, phương tiện truyền thông cung cấp các nội dung thông tin được cập nhật định kỳ |
| 4330 | Hoàn thiện công trình xây dựng |
| 7310 | Quảng cáo |

Những ngành nghề kinh doanh của Công ty ....................................................... phù hợp với loại hình dịch vụ và nội dung thông tin dự định cung cấp trên mạng xã hội .................. Cụ thể như sau:

Để phù hợp với loại hình dịch vụ: “Tạo trang thông tin điện tử cá nhân, diễn đàn (forum), trò chuyện (chat) trực tuyến, chia sẻ âm thanh, hình ảnh” và nội dung thông tin dự định cung cấp là: thảo luận, trao đổi các thông tin về âm nhạc, Công ty ....................................................... có đăng ký kinh doanh ngành nghề:

Cổng thông tin

Chi tiết: Hoạt động điều hành các website sử dụng công cụ tìm kiếm để tạo lập và duy trì các cơ sở dữ liệu lớn các địa chỉ internet và nội dung theo một định dạng có thể tìm kiếm một cách dễ dàng Hoạt động điều hành các website khác hoạt động như các cổng internet, như các trang báo chí, phương tiện truyền thông cung cấp các nội dung thông tin được cập nhật định kỳ.

**2.3. Thông tin khái quát về mạng xã hội:**

a) Tên miền: .................

b) Tổ chức thiết lập website: Công ty .......................................................

c) Địa chỉ trụ sở chính:

          Điện thoại:                               Email:

d) Người chịu trách nhiệm chính:

Sinh năm:

Nơi đăng ký hộ khẩu thường trú:

CMND số:                     cấp tại                  ngày     tháng    năm

- Chức vụ: Quản lý nội dung

- Số điện thoại liên lạc (cố định và di động):

Cố định :                                    Di động :

**2.4. Điều kiện về tên miền**

Công ty ................................. sử dụng tên miền ................. đáp ứng điều kiện về tên miền quy định tại điểm a, b, c khoản 3 Điều 5 Thông tư 09/...../TT-BTTTT Quy định chi tiết về hoạt động quản lý, cung cấp, sử dụng thông tin trên trang thông tin điện tử và mạng xã hội. Cụ thể như sau:

- Công ty ....................................................... không phải là cơ quan báo chí cho nên dãy ký tự tạo nên tên miền ................. không giống hoặc trùng với tên cơ quan báo chí nào

- Trang thông tin điện tử tổng hợp của Công ty ....................................................... không sử dụng cùng một tên miền

- Mạng xã hội ................. sử dụng ít nhất một tên miền “.vn” và lưu giữ thông tin tại hệ thống máy chủ có địa chỉ IP ở Việt Nam. Thực hiện đúng quy định tại Điều 7, Thông tư 24/2015/TT-BTTTT quy định về quản lý và sử dụng nguồn tài nguyên Internet

- Cơ sở pháp lý để thành lập mạng xã hội

- Các văn bản pháp luật có liên quan khác.

Phương thức tổ chức mạng xã hội, các loại hình dịch vụ và phạm vi lĩnh vực thông tin trao đổi

- Phương thức tổ chức mạng xã hội, các loại hình dịch vụ, phạm vi, lĩnh vực thông tin trao đổi

- Phương thức tổ chức mạng xã hội: phương thức trực tuyến

- Loại hình dịch vụ: Tạo trang thông tin điện tử cá nhân, diễn đàn (forum), trò chuyện (chat) trực tuyến, chia sẻ âm thanh, hình ảnh

- Phạm vi thông tin trao đổi: Mạng Internet

- Lĩnh vực thông trao đổi: Mạng xã hội chia sẻ thông tin trên mạng internet về âm nhạc

- Các chuyên mục dự kiến của mạng xã hội trực tuyến .................

Là một website cung cấp dịch vụ mạng xã hội trực tuyến thuần Việt được thể hiện cụ thể qua một giao diện thân thiện, dễ dàng sử dụng và truy cập với tốc độ nhanh, giao diện đồ họa đảm bảo tính tiện dụng, mỹ thuật, bố cục đơn giản, màu sắc ấn tượng. Về ngôn ngữ, sử dụng tiếng Việt trong sáng, cho phép người dùng có thể phát huy được sự sáng tạo và thể hiện cá tính của mình. www........ được xây dựng hoàn toàn mới với ứng dụng giao diện chuẩn web với các chức năng chính như Trang chủ, Thể loại, Bảng xếp hạng, Video Clip, Diễn đàn, Nhạc cá nhân, Nghệ sĩ, Upload.

Các chuyên mục chính dự kiến của .................:

Trang chủ: Tổng quan về trang web, cung cấp cho bạn đọc cái nhìn tổng quát nhất về cấu trúc và chức năng của website

Diễn đàn: Là chuyên mục để các thành viên về các hoạt động liên quan đến âm nhạc

Nhạc cá nhân: Là chuyên mục để các thành viên tự tạo danh sách nghe nhạc theo sở thích cá nhân dựa trên các bản nhạc của mạng xã hội.

Đăng nhập: Là chuyên mục cung cấp giao diện giúp người dùng đăng nhập vào hệ thống và trở thành thành viên của mạng xã hội ................. bao gồm tên đăng nhập, mật khẩu

Đăng ký: Là chuyên mục cung cấp giao diện để người dùng đăng ký trở thành thành viên của mạng xã hội .................

Điều khoản – Thỏa thuận: Là chuyên mục quy định nội quy sử dụng mạng xã hội, quyền và nghĩa vụ của các bên khi tham gia.

- Phương án tổ chức nhân sự, kỹ thuật, tài chính nhằm bảo đảm hoạt động của mạng xã hội .................

- Phương án tổ chức nhân sự trong mạng xã hội trực tuyến

- Biện pháp quản lý nội dung

Công ty ....................................................... đã thành lập bộ phận quản lý nội dung thông tin để quản lý mạng xã hội ................. đáp ứng yêu cầu quy định tại Điểm đ, khoản 1 Điều 3 Thông tư 09/2014/TT-BTTTT Quy định chi tiết về hoạt động quản lý, cung cấp, sử dụng thông tin trên trang thông tin điện tử và mạng xã hội. Bộ phận gồm 6 người, có trách nhiệm kiểm tra, rà soát thông tin, nội dung thông tin trên diễn đàn, đảm bảo tất cả nội dung đăng trên diễn đàn không vi phạm thỏa thuận, không vi phạm pháp luật, không trái đạo đức xã hội. Khi phát hiện sai phạm về nội dung bộ phận này có toàn quyền quyết định hình thức xử lý thành viên từ nhắc nhở đến đưa ra cơ quan pháp luật giải quyết

* Người chịu trách nhiệm chính:

Chức vụ:

Tốt nghiệp chuyên ngành:

Phụ trách hoạch địch và quản lý chung, kiểm tra các thông tin được đăng tải trên mạng xã hội và xử lý các tình huống phát sinh.

* Quản trị mạng xã hội (03 người) :

- …………………… - Nhân viên nội dung

- …………………… - Nhân viên quản lý tin bài

- …………………… - Nhân viên quản lý nguồn tin

Quản lý thông tin đăng ký của thành viên, quản lý tin bài, kiểm duyệt thông tin người dùng đưa lên, quản lý nội dung trò chuyện thảo luận giữa các thành viên, quản lý nguồn tin do các thành viên chia sẻ trên mạng xã hội

* Bộ phận kỹ thuật (02 người):
1. …………………………………….

Chức danh: Nhân viên kỹ thuật

         Trình độ chuyên môn: Đại học

1. ………………………………………

Chức danh: Nhân viên kỹ thuật

Trình độ chuyên môn:

Phụ trách việc phát triển mạng xã hội về mặt kỹ thuật, đảm bảo trang mạng xã hội hoạt động ổn định và bí mất

Đáp ứng quy định tại điểm g, điểm h khoản 2 Điều 2 Thông tư 03/2014/TT-BTTTT ngày 11 tháng 3 năm 2014 của Bộ Thông tin và Truyền thông ban hành chuẩn kỹ năng sử dụng công nghệ thông tin.

* Đáp ứng mô đun kỹ năng 13 ( Mã IU13) biên tập trang thông tin điện tử

+ Hiểu khái niệm ứng dụng web. Biết phân biệt web với các dịch vụ Internet hỗ trợ khác (Ví dụ: truyền tệp, thư điện tử, nhắn tin).

+ Hiểu khái niệm máy chủ web (web server), trình duyệt (browser) và sự tương tác giữa chúng. Hiểu các khái niệm miền (domain), URL (Uniform Resource Locator), siêu liên kết, thuê máy chủ web (web hosting), bộ tìm kiếm (search engine).

+ Biết khái niệm giao thức (protocol). Phân biệt các giao thức TCP/IP, HTTP, FTP.

+ Hiểu khái niệm xuất bản trang web (webpage), website. Biết các công việc cần làm để sở hữu một website (đăng ký tên miền, chọn dịch vụ thuê máy chủ).

+ Biết các bước để xây dựng một website như hoạch định, thiết kế, cập nhật nội dung, tải lên máy chủ web, phát hành và bảo trì. Biết các nhân tố quan trọng tạo nên một website hiệu quả như hỗ trợ tìm kiếm, hỗ trợ tải nội dung.

+ Biết các kỹ thuật tối ưu hóa trình tìm kiếm trên website như siêu dữ liệu, sơ đồ cấu trúc của website và liên kết website.

+ Biết các nhân tố ảnh hưởng đến tốc độ tải xuống một trang web. Nhận biết các định dạng tệp âm thanh, video, đồ họa phù hợp để tối ưu hóa tốc độ tải xuống

+ Hiểu thuật ngữ bản quyền (copyright) đối với các nội dung trên các website.

+ Hiểu cần phải tuân thủ các quy định của luật pháp nơi website được đặt đối với việc đăng tải nội dung trên website.

+ Hiểu khái niệm HTML (HyperText Markup Language) – ngôn ngữ để viết mã nguồn của một ứng dụng web. Hiểu khái niệm thẻ đánh dấu (tag) và công dụng. Biết cú pháp của một câu lệnh HTML. Biết về Liên minh W3C (World Wide Web consortium) và các khuyến nghị phát triển HTML của W3C

+ Biết sử dụng các thẻ đánh dấu để cấu trúc việc trình bày một trang web (<html>, <head>, <title>, <body>) và để thể hiện một trang web (<h1>, <h2>, <p>, <br>, <a>, <img>).

+ Biết quy trình và các kỹ thuật để hoạch định và thiết kế website (xác định đối tượng phục vụ chính và phân tích, đánh giá nhu cầu của đối tượng này, xây dựng các kịch bản tìm kiếm và khai thác thông tin, lập sơ đồ cấu trúc của website, sơ đồ tìm kiếm).

+ Biết sử dụng các phần mềm ứng dụng làm website. Biết sử dụng phần trợ giúp của phần mềm này

+ Biết tạo, ghi trang web, website mới tạo lên thiết bị lưu trữ. Biết cách sử dụng các trang web mẫu để tạo trang web.

+ Biết biên tập tên trang web

+ Biết cách sử dụng trình duyệt để xem mã nguồn dạng HTML của một trang web. Biết chuyển qua lại giữa mã nguồn và trang web.

+ Hiểu cách đặt các thông số chính trong phần mềm phát triển web như trình duyệt mặc định dùng xem trước nội dung, cách mã hóa, phông chữ mặc định. Biết các kinh nghiệm tốt khi trình bày (ví dụ: chọn phông chữ).

+ Biết cách nhập, biên tập, xóa văn bản.

+ Biết các cách định dạng phông chữ như tên, cỡ, đậm, nghiêng, kiểu dáng và màu.

+ Biết cách chọn một đoạn, cách đưa vào/loại bỏ các dấu ngắt đoạn, ngắt dòng.

+ Biết các cách định dạng đoạn như đặt lề, thụt dòng, đánh số, đánh dấu đầu dòng (bullet).

+ Biết cách định dạng một trang web, cách đặt lề, xử lý màu nền, ảnh nền.

+ Hiểu khái niệm siêu liên kết (hyperlink), phân biệt siêu liên kết tuyệt đối và tương đối.

+ biết nhập, biên tập và hủy một siêu liên kết thông thường, một siêu liên kết thư điện tử.

+ Biết cách xác định đích của siêu liên kết trên cùng cửa sổ, khác cửa sổ.

+ Biết cách thay đổi màu siêu liên kết truy cập (visited), không truy cập (unvisited), hoạt động (active).

+ Biết khái niệm và cách sử dụng neo (anchor)

-        Đáp ứng môn đun kỹ năng 14, an toàn và bảo mật thông tin

+ Biết phân biệt giữa dữ liệu và thông tin. Biết cách thức lưu trữ, vận chuyển dữ liệu và thông tin trong môi trường truyền thông

+ Hiểu các loại nguy cơ đối với dữ liệu: mất cắp, mất an toàn (safety) về vật lý (hư hỏng môi trường lưu giữ, các thảm họa - chiến tranh, thiên tai, cháy nổ), không đảm bảo an toàn thông tin trong khai thác, sử dụng. Sau đây là một số phương thức bảo đảm an toàn, bảo mật thông tin, dữ liệu: Mật mã (Cryptography): là việc thực hiện chuyển đổi dữ liệu theo một quy tắc nào đó thành dạng mới mà kẻ tấn công không nhận biết được.Xác thực (Authentication): là các thao tác để nhận dạng người dùng, nhận dạng client hay server… Ủy quyền (Authorization): chính là việc phân định quyền hạn cho mỗi thành phần đã đăng nhập thành công vào hệ thống. Quyền hạn này là các quyền sử dụng dịch vụ, truy cập dữ liệu…Kiểm toán (Auditing): là các phương pháp để xác định được client đã truy cập đến dữ liệu nào và bằng cách nào.

+ Hiểu nguồn gốc các nguy cơ đối với việc đảm bảo an toàn thông tin: từ nhân viên, các nhà cung cấp dịch vụ, từ các cá nhân bên ngoài. Hiểu khái niệm tội phạm mạng (cybercrime).

+ Biết các điểm yếu của máy tính cá nhân (lây nhiễm virus và các phần mềm độc hại - malware).

+ Biết về các lỗ hổng bảo mật hệ thống: của hệ điều hành, hệ quản trị cơ sở dữ liệu, dịch vụ Internet. Biết các khái niệm và phương thức hoạt động của các thiết bị bảo mật và phân biệt việc đảm bảo an toàn cho tổ chức như chính phủ, doanh nghiệp và đảm bảo an toàn cho cá nhân khi tham gia các hoạt động trên mạng.

+ Biết các đặc trưng cơ bản của an toàn thông tin: tính mật, tính toàn vẹn, tính sẵn sàng, tính xác thực.

+ Biết các quy định phổ biến về bảo vệ, gìn giữ và kiểm soát dữ liệu, sự riêng tư tại Việt Nam.

+ Hiểu vai trò của các lĩnh vực liên quan đến an toàn dữ liệu: chính sách, tổ chức, biện pháp quản lý và các giải pháp công nghệ.

+ Biết về tiêu chuẩn TCVN ISO/IEC 27001:2009. Biết một số chính sách cơ bản về an toàn thông tin và một số văn bản pháp luật về an toàn thông tin của Việt Nam. Hiểu tầm quan trọng của việc xây dựng và thi hành chính sách an toàn thông tin đối với việc ứng dụng CNTT.

+ Hiểu cách virus thâm nhập vào máy tính (ví dụ: khi sao chép các tệp vào máy tính, khi mở thư điện tử và các tệp đính kèm thư). Biết cách chủ động phòng, tránh virus cho máy tính cá nhân như tuân thủ chặt chẽ các quy tắc kiểm soát khi sao chép các tệp lạ, cài đặt phần mềm; sử dụng các phần mềm chống virus, phần mềm an ninh mạng đúng cách.

+ Hiểu tác dụng và hạn chế chung của phần mềm diệt virus, phần mềm an ninh mạng. Biết cách sử dụng hiệu quả các phần mềm diệt virus, phần mềm an ninh mạng và cập nhật thường xuyên các phần mềm này. Ngoài ra Sao lưu dữ liệu theo chu kỳ là biện pháp đúng đắn nhất hiện nay để bảo vệ dữ liệu. Bạn có thể thường xuyên sao lưu dữ liệu theo chu kỳ đến một nơi an toàn như: các thiết bị nhớ mở rộng (ổ USB, ổ cứng di động, ghi ra đĩa quang...), hình thức này có thể thực hiện theo chu kỳ hàng tuần hoặc khác hơn tuỳ theo mức độ cập nhật, thay đổi của dữ liệu của bạn.

Tạo các dữ liệu phục hồi cho toàn hệ thống không dừng lại các tiện ích sẵn có của hệ điều hành (ví dụ System Restore của Windows Me, XP...) mà có thể cần đến các phần mềm của hãng thứ ba, ví dụ có thể tạo các bản sao lưu hệ thống bằng các phần mềm ghost, các phần mềm tạo ảnh ổ đĩa hoặc phân vùng khác.

+ Hiểu về thông tin cá nhân: thông tin định danh (identity), tài khoản cá nhân (tên người dùng, mật khẩu truy nhập); thông tin cá nhân, tài chính, kinh doanh, pháp lý và một số chi tiết liên quan đến cá nhân có thể bị lợi dụng, xâm hại khác.

+ Hiểu cách thức thông tin cá nhân được sử dụng: để truy nhập vào máy tính, vào tệp, vào mạng và khai báo trong các giao dịch trên mạng

+ Hiểu cách thông tin cá nhân có thể bị lấy cắp thông qua các phần mềm độc dùng để lấy cắp dữ liệu phần mềm quảng cáo (adware), gián điệp (spyware), botnet, dò gõ phím (keystroke logging), quay số (dialler) và các phần mềm tương tự.

+ Biết một số hành vi tội phạm như thu thập trái phép thông tin, lừa đảo, truy nhập trái phép vào hệ thống máy tính. Biết một số phương thức thực hiện các hành vi phạm tội này như cuộc gọi qua điện thoại, lừa đảo (phishing), nhìn lén thông tin (shoulder surfing).

+ Biết cách phòng chống mất cắp thông tin cá nhân và phòng chống lừa đảo, lợi dung trên mạng cơ bản như không cung cấp thông tin nhạy cảm, cảnh giác với các giao dịch lạ, áp dụng mật mã đối với các thông tin nhạy cảm.

+ Biết tầm quan trọng và hiệu quả của việc thiết lập chế độ an toàn chung (macro security settings).

+ Biết tầm quan trọng và cách đặt mật khẩu đối với tệp, tệp tin nén

+ Hiểu một số biện pháp mã hóa dữ liệu. Biết các ưu điểm và hạn chế khi sử dụng mật mã (encryption) đối với tài liệu

+ Biết một số phương thức tấn công mạng chủ yếu của tin tặc (hacker) như trinh sát, dò quét, tấn công vào các điểm yếu, sử dụng các lỗ hổng an toàn. Biết về một số dạng tấn công phổ biến qua mạng Internet chính như tấn công từ chối dịch vụ (DOS), botnet

+ Biết về các cơ chế và công nghệ chống lại tấn công trên mạng như phân vùng mạng, mạng riêng ảo (VPN), một số hệ thống bảo vệ phổ biến (ví dụ: tường lửa). Hiểu chức năng và giới hạn của tường lửa.

+ Biết các công nghệ bảo vệ hệ thống cơ bản như đăng nhập, kiểm soát truy nhập, quản trị mật khẩu, quản trị người sử dụng, khai thác tệp tin hồ sơ truy nhập (log).

+ Hiểu các chế độ đảm bảo an toàn của mạng: kiểm soát phần mềm độc, kiểm soát truy nhập trái phép dữ liệu, đảm bảo tính riêng tư (maintaining privacy). Biết cách kết nối với một mạng có các chế độ đảm bảo an toàn đó.

+ Biết ưu/nhược điểm của các phương thức kết nối với một mạng (cáp, không dây). Biết các vấn đề liên quan đến bảo mật mạng không dây. Biết các nguy cơ bị nghe trộm và đánh cắp dữ liệu từ mạng không dây.

+ Hiểu tầm quan trọng của việc bảo vệ mật khẩu truy cập cho mạng không dây. Biết cách kết nối với một mạng không dây được bảo vệ/không được bảo vệ

+ Biết các phương pháp bảo mật cho mạng không dây như WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA2 (Wi-Fi Protected Access 2), MAC (Media Access Control).

+ Biết nguyên lý và các kiến trúc hệ thống để phát hiện và chống xâm nhập trái phép. Biết các kỹ thuật phát hiện và ngăn chặn xâm nhập trái phép

+ Hiểu được mục đích của một tài khoản mạng và biết cách sử dụng nó để truy cập mạng.

+ Biết cách vận dụng các chính sách mật khẩu tốt (không chia sẻ mật khẩu, thay đổi thường xuyên, đảm bảo chiều dài mật khẩu, mật khẩu có đầy đủ chữ, số và ký tự đặc biệt).

+ Biết về các giải pháp bảo mật sử dụng công nghệ sinh trắc học trong kiểm soát truy cập như dấu vân tay, quét mắt.

+ Hiểu sự cần thiết khi thực hiện các giao dịch trực tuyến (mua hàng, giao dịch tài chính) trên các trang web an toàn.

+ Biết các dấu hiệu của một trang web an toàn như https, biểu tượng khóa.

+ Biết khái niệm xác thực số. Hiểu lợi ích của mật khẩu dùng một lần

+ Biết cách sử dụng chế độ tự động hoàn chỉnh, tự động lưu khi soạn thảo một biểu mẫu khai trên mạng

+ Biết cách xóa dữ liệu cá nhân từ một trình duyệt như lịch sử duyệt web (browsing history), các tệp Internet được lưu (cached Internet files), mật khẩu (password), cookies, các dữ liệu tự điền (autocomplete data).

+ Hiểu thuật ngữ cookie và biết cách chọn các cài đặt thích hợp để cho phép hoặc ngăn chặn cookie.

+ Hiểu được mục đích, chức năng một số loại phần mềm kiểm soát nội dung như phần mềm lọc Internet, phần mềm kiểm soát truy nhập Internet.

+ Hiểu biết về mối nguy hiểm tiềm năng khi sử dụng các trang mạng xã hội. Hiểu được tầm quan trọng của việc không tiết lộ thông tin bí mật trên các trang web mạng xã hội.

+ Hiểu sự cần thiết phải áp dụng các đặc tính riêng tư cho tài khoản mạng xã hội

+ Hiểu mục đích của việc mã hóa, giải mã đối với thư điện tử (e-mail).

+ Hiểu thuật ngữ chữ ký số. Biết cách tạo và điền một chữ ký số vào thư điện tử

+Nhận biết nguy cơ từ các thư điện tử không không rõ nguồn gốc

+ Biết khái niệm lừa đảo (phishing). Biết các đặc điểm chung của lừa đảo như dùng tên của các công ty, cá nhân hợp pháp, các liên kết web không đúng

+ Biết mối nguy hiểm đối với máy tính khi mở thư có đính kèm phần mềm độc. Biết cách phòng ngừa khi mở các thư có đính kèm các tệp đáng nghi

+ Hiểu biết về các lỗ hổng bảo mật đối với tin nhắn tức thời (IM) như phần mềm xấu, truy nhập theo lối cửa sau (backdoor access).

+ Biết cách áp dụng các phương pháp bảo mật khi dùng nhắn tin như dùng mật mã, không để lộ thông tin quan trọng, hạn chế chia sẻ tệp.

+ Biết ưu nhược điểm của các phương pháp hủy dữ liệu vĩnh viễn phổ biến như phá ổ đĩa, dùng công cụ phá hủy.

+ Biết khái niệm sao lưu (backup) dữ liệu và tầm quan trọng của việc này. Biết các chế độ sao lưu và vai trò của chúng như sao lưu thường xuyên, theo lịch, theo địa điểm

+ Biết cách sao lưu dữ liệu

+ Biết cách khôi phục dữ liệu sao lưu và xác nhận dữ liệu

+ Hiểu được lý do xóa dữ liệu vĩnh viễn từ ổ đĩa hoặc các thiết bị lưu trữ khác

+ Phân biệt giữa việc xóa dữ liệu và hủy dữ liệu vĩnh viễn

+  Các cách bảo vệ vật lý cho thiết bị như khóa vị trí và chi tiết về thiết bị, khóa cáp (cable locks), kiểm soát tiếp cận vật lý.

1. Phương án kỹ thuật
	* Khái quát chung về hạ tầng kỹ thuật

+ HDD: Volume 2000 SAS

+ Ram: 2GB

+ Băng thông: 100GB

Hạ tầng kỹ thuật bao gồm các máy tính, thiết bị mạng, hệ điều hành, phần mềm hệ thống và phần mềm chuyên dụng để quản lý, khai thác, sử dụng mạng, bảo vệ an ninh an toàn mạng, đặc biệt là các phần mềm ứng dụng giá trị nội dung, cửa sổ dữ liệu cho website. Hạ tầng kỹ thuật của Công ty ....................................................... đảm bảo được các yếu tố sau :

* Sử dụng các công nghệ mạng, truyền thông và máy tính tiên tiến nhất hiện nay trong quá trình tích hợp hệ thống để xây dựng một hệ thống mạng máy chủ dịch vụ, website mạnh đáp ứng tốt mọi yêu cầu của người truy cập dịch vụ, dễ dàng kết nối với mạng Internet quốc gia, quốc tế.
* Tính ổn định: Hệ thống được thiết kế đảm bảo khả năng hoạt động liên tục có dự phòng về máy chủ đảm bảo khả năng khôi phục dữ liệu và thay thế nóng trong mọi trường hợp.
* Độ tin cậy (tính bảo mật của hệ thống): Đảm bảo độ tin cậy với việc sử dụng các giao thức chuẩn tiên tiến nhất hiện nay và các thiết bị của những hãng có tên tuổi và uy tín trên thế giới.
* An ninh mạng và thông tin trên mạng: áp dụng các giải pháp đảm bảo an toàn an ninh mạng bằng việc sử dụng giải pháp Firewall, các thiết bị kiểm soát chống truy nhập bất hợp pháp. Phối hợp với các cơ quan chức năng áp dụng các quy định của nhà nước về việc cung cấp thông tin trên Internet, các quy trình kiểm tra kiểm soát dịch vụ.

2.2 Giải pháp lưu trữ

* Hệ thống hoạt động có sự backup đầy đủ về mặt kỹ thuật, Lưu trữ tối thiểu 02 (hai) năm đối với các thông tin về tài khoản, thời gian đăng nhập, đăng xuất, địa chỉ IP của người sử dụng và nhật ký xử lý thông tin được đăng tải.
* Phần mềm lưu trữ: Hệ quản trị cơ sở dữ liệu MySQL Server 5.5
* Phương thức lưu trữ: Lưu trữ theo tuần. Dữ liệu chính vẫn được lưu online trên hệ thống, mỗi tuần sẽ được backup 1 bản phụ về server backup.

2.3 Cơ chế tiếp nhận và xử lý cảnh báo thông tin vi phạm:

* Tiếp nhận và xử lý cảnh báo thông tin vi phạm từ người sử dụng. Đảm bảo ngăn chặn và loại bỏ các thông tin vi phạm quy định tại điều 5 Nghị định 72/2013/NĐ-CP chậm nhất sau 03 (ba) giờ kể từ khi tự phát hiện hoặc khi có yêu cầu của cơ quan nhà nước có thẩm quyền.
* Hệ thống phần mềm có tính năng báo cáo vi phạm, được hiển thị phía dưỡi mỗi bài viết do thành viên đưa lên. Nếu người sử dụng phát hiện thông tin sai phạm, người sử dụng chỉ cần thao thác bằng cách ấn vào nút báo cáo vi phạm. Các thông tin vi phạm sẽ được Ban quản trị tiếp nhận thông qua link “báo cáo vi phạm”, hoặc do các thành viên phát hiện và gửi mail báo về vi phạm đó. Sau khi tiếp nhận các thông tin có dấu hiệu vi phạm Ban quản trị sẽ tiến hành rà soát lại những thông tin bị phản ảnh sai phạm, quản trị viên sẽ tiến hành gỡ bỏ bài viết khỏi hệ thống đồng thời phân loại mức độ vi phạm của từng thông tin cụ thể để đưa ra biện pháp xử lý phù hợp. Tùy theo mức độ vi phạm mà có thể bị xử lý như cảnh báo, tạm khóa tài khoản, xóa vĩnh viển tài khoản
* Đối với các thông tin do Ban quản lý phát hiện vi phạm hoặc được các thành viên khác “báo cáo vi phạm” , và được Ban quan lý kiểm chứng thông tin báo cáo vi phạm là đúng, Ban quản lý sẽ gửi thông báo cảnh báo nội dung vi phạm và yêu cầu thành viên vi phạm ngay lập tức gỡ bỏ nội dung thông tin vi phạm đó. Nếu thành viên không gỡ bỏ nội dung vi phạm, Ban quan trị sẽ tiến gỡ bỏ, xóa nội dung và buộc sẽ tạm khóa tài khoản của thành viên vi phạm. Nếu vi phạm 03 lần Ban quan trị buộc lòng xóa vĩnh viễn tài khoản bạn. Đồng thời chúng tôi sẽ thông báo cho bạn qua email của thành viên vi phạm. Thành viên cũng có thể xóa tài khoản của mình hoặc làm vô hiệu ứng dụng của mình bất kỳ lúc nào.
* Những bài viết, thông tin đưa lên mạng xã hội với mục đích quấy rối, hạ thấp uy tín Ban quản trị sẽ bị cảnh cáo khóa tài khoản.
* Nếu thành viên nào tham gia diễn đàn với mục đích phá hoại sẽ bị khóa tài khoản cho dù chưa gửi bài nào trên diễn đàn.
* Nếu thành viên lợi dụng diễn đàn đề chia sẽ trao đổi những nội dung bị cấm trao đổi hoặc trao đổi, chia sẽ các nội dung quy định tại điều 5 Nghị định 72/2013/ND-CP thì bị xóa tài khoản vĩnh viễn và sẽ không cho phép sử dụng các thông tin đăng ký của tài khoản bị xóa để tạo tài khoản khác. Trong trường hợp vi phạm thì thành viên phải chịu trách nhiệm về các hành vi của mình trước pháp luật.
* Trong trường hợp thông tin do thành viên cung cấp cho Mạng xã hội ................. không chính xác, sai lệch, không đầy đủ hoặc vi phạm pháp luật hay thuần phong mỹ tục Việt Nam, vi phạm các quy định của thỏa thuận này, vi phạm quy định của pháp luật có liên quan thì Ban Quản lý có quyền từ chối, tạm ngừng hoặc chấm dứt tư cách và quyền sử dụng dịch vụ của thành viên.

2.4 Cơ chế phát hiện, cảnh báo, ngăn chặn truy nhập bất hợp pháp, các hình thức tấn công trên môi trường mạng và tuân theo những tiêu chuẩn đảm bảo an toàn thông tin

Server :

* Các server nội bộ được đặt local IP, bật firewall. Muốn truy cập các server này phải thông qua 1 proxy server. Trên proxy server bật firewall, chỉ mở port SSH cho truy cập từ xa. Để truy cập proxy server phải có key SSH hợp lệ được cấp bởi system admin.
* Tất cả các server được đặt password phức tạp (trên 8 ký tự, chữ hoa + chữ thường + số + ký tự đặt biệt); dùng phần mềm KeePass gen pasword
* Thường xuyên kiểm tra Log để check các truy cập không hợp lệ .

      Network:  Trên router chỉ mở các port như sau:

* Proxy server : port 22 cho SSH.
* Web server  : port 80 and 443.
* Cấu hình password trên router phải được mã hóa , password phải đảm bảo phức tạp như cách đặt password cho server.
* Hệ thống Mạng xã hội ................. được tổ chức và vận hành một cách hợp lý để đảm bảo tránh được khả năng tấn công leo thang. Hệ thống phòng vệ tường lửa (firewall); công cụ phát hiện, phòng chống xâm nhập, tấn công;… được Mạng xã hội  .................  sử dụng để bảo vệ an toàn, an ninh thông tin của Người dùng và hệ thống.
* Thông tin được lưu mã hóa vào database, và được bảo vệ bằng mật khẩu 128bit để đảm bảo các thông tin nhạy cảm. Thông tin cá nhân của Người dùng như số CMND, địa chỉ được bảo mật tuyệt đối.
* Hệ thống được cài đặt phần mềm chống vi rút Anti Virus được chạy độc lập nhằm hạn chế sự xâm nhập của virus, cũng như các phương thức tấn công nội bộ (local hack); đảm bảo cho sự vận hành liên tục của hệ thống, hạn chế lỗi, đảm bảo lưu trữ, an toàn và an ninh thông tin. Anti Virus có các tính năng ưu việt như sau:
* Hỗ trợ quét virut theo thời gian thực;
* Quét nhanh, daemon đa luồng với sự hỗ trợ cho việc quét vùng truy cập;
* Cơ sở dữ liệu vi rút nhiều và cập nhật mới liên tục;
* Tích hợp hỗ trợ cho các định dạng lưu trữ khác nhau, bao gồm cả Zip, RAR, TAR, GZIP, BZIP2, OLE2, và các định dạng khác.
* Cách thức ngăn chặn và diệt vi rút của phần mềm Anti Virus:
1. Phương pháp thứ nhất:
* Kiểm tra (quét) các tập tin để phát hiện các vi rút đã biết trong cơ sở dữ liệu nhận dạng về vi rút.
* Để kiểm tra và phát hiện vi rút thì phần mềm dùng phương pháp so sánh mẫu trong cơ sở dữ liệu nhận biết vi rút. Các tập tin cần kiểm tra vi rút được phân tích và so sánh với các mẫu vi rút đã biết trước, nếu phát hiện một đoạn mã vi rút thì tập tin đó có thể bị lây nhiễm vi rút và phần mềm thực hiện biện pháp loại bỏ vi rút khỏi tập tin bị lây nhiễm.
1. Phương pháp thứ hai:
* Phát hiện các hành động của các phần mềm giống như các hành động của vi rút hoặc các phần mềm độc hại.
* Phần mềm diệt vi rút sẽ theo dõi sự hoạt động bất thường của hệ thống để có thể phát hiện các vi rút chưa được biết đến (trong dữ liệu của nó) hoặc các phần mềm độc hại để từ đó đưa ra cảnh báo người sử dụng, cô lập vi rút để sẵn sàng gửi mẫu đến hãng bảo mật phân tích và cập nhật vào bản nâng cấp cơ sở dữ liệu kế tiếp.
* Trên hệ thống máy chủ của Mạng xã hội ................. phần mềm diệt vi rút sẽ thực hiện kiểm soát liên tục theo thời gian thực để bảo vệ hệ thống. Hình thức kiểm soát liên tục sẽ quét vi rút mọi tập tin mà hệ thống truy cập đến, mọi tập tin ngay từ khi bắt đầu được chép vào hệ thống thông qua hình thức nhận biết so sánh mẫu và theo dõi hành động đáng ngờ.
* Luôn có một máy chủ (server) chạy song song với server chính để sao lưu dự phòng dữ liệu, và có khả năng phục hồi dữ liệu ngay khi máy chủ chính gặp sự cố.
* Khi hệ thống phát hiện truy cập bất hợp pháp (truy cập hàng loạt, cố gắng truy cập nhiều lần vào các nội dung bị khóa mật khẩu - mục đích dò mật khẩu,... ) thì các truy cập này sẽ bị chặn (chặn IP).
* Người dùng được cung cấp username (Người dùng tự chọn) và mật khẩu để đăng nhập hệ thống, thông tin về mật khẩu được mã hóa để đảm bảo không ai (ngay cả nhân viên của Mạng xã hội ................. có thể biết được ngoại trừ Người dùng.
* Chỉ những nơi có IP (IP tĩnh như IP văn phòng của Mạng xã hội ................. được cấp quyền, và phải có mật khẩu mới có thể truy cập vào hệ thống quản lý, giúp giảm tối đa rủi ro truy cập vào hệ thống quản lý bất hợp pháp.
* Trước khi Mạng xã hội ................. được đưa vào sử dụng và trong suốt quá trình vận hành Mạng xã hội ................., Công ty cùng với đội ngũ nhân sự của mình thường xuyên kiểm tra, rà soát các vấn đề liên quan đến bảo mật, an toàn của hệ thống. Các vấn đề được kiểm tra, rà soát như:
* Rà soát về phần cứng và kết nối:

+ Kiểm tra trực tiếp các thông số, khả năng hoạt động thực tế của các máy chủ; kiểm tra khả năng hỗ trợ nhau của các máy chủ.

+ Kiểm tra kết nối mạng, yêu cầu nhà cung cấp mạng cung cấp đường truyền đúng thỏa thuận giữa các bên, đảm bảo vận hành liên tục của hệ thống.

+ Rà soát về việc cung cấp các tiện ích Mạng xã hội .................. Kiểm tra việc thiết kế, lập trình các tiện ích được cung cấp bởi Mạng xã hội ................. việc kết nối các tiện ích vào hệ thống.

+ Rà soát về phần mềm:Phần mềm và việc lập trình của hệ thống không cho phép Người dùng có thể can thiệp vào quá trình redirect từ ứng dụng này sang ứng dụng khác. Việc redirect từ ứng dụng này sang ứng dụng khác được thực hiện trong khuôn khổ các ứng dụng đã được lập trình sẵn.

+ Hệ thống yêu cầu Người dùng dùng mật khẩu đủ mạnh để tránh trường hợp mật khẩu của Người dùng bị tấn công.

+ Khi Người dùng đăng nhập, hệ thống sẽ làm mới các session của Người dùng trong các đăng nhập cũ. Ngay khi Người dùng thoát đăng nhập khỏi Mạng xã hội ................. , các session của Người dùng sẽ bị xóa.

+ Đảm bảo các ứng dụng web khi gặp lỗi không bị lộ thông tin hệ thống.

+ Kiểm tra dữ liệu đầu vào nhằm đảm bảo đó không phải là một hình thức tấn công hoặc lây truyền vi rút.

* Đội ngũ nhân sự của Mạng xã hội... được đào tạo bài bản về chuyên môn, nghiệp vụ, từ đó có đủ năng lực để vận hành hệ thống tốt nhất, đảm bảo an toàn, an ninh thông tin..

**2.5. Phương án dự phòng đảm bảo duy trì hoạt động an toàn, liên tục và khắc phục khi có sự cố xảy ra.**

Máy chủ:

* Web server : tối thiểu 2 server web cho site .
* Database : tối thiểu 2 server db (master + slave) .
* File server : tối thiểu 2 server
* Backup file config của các server thường xuyên. Khi có sự cố thì khôi phục lại 1 cách nhanh chóng .

Hệ thống mạng:

* Phải có ít nhất 2 thiết bị router với cấu hính giống nhau phòng khi router chính bị lỗi thì bật router phụ lên thay thế .
* Backup file cấu hình của thiết bị thường xuyên, khi có sự cố có thể khôi phục lại cấu hình nhanh chóng.
* Gửi email cho bộ phận kỹ thuật khi có sự cố xảy ra

Nhân sự:  Luôn có bộ phận kỹ thuật trực 24/7, trong trường hợp sự cố xảy ra có thể can thiệp ngay sau 30 phút

**2.6. Giải pháp bảo đảm an toàn an ninh thông tin mạng**

Bảo mật thông tin và an ninh mạng là yêu cầu quan trong trong quá trình tổ chức, xây dựng trang mạng xã hội nhằm chống sự xâm nhập bất hợp pháp của các đối tượng phá hoại (hacker), chống virus, đảm bảo cho trang mạng xã hội hoạt động bình thường, do vậy ................. đã đặt ra yêu cầu đối với  các vấn đề này như sau:

* Dùng các phần mềm anti- virus trên tất cả các máy.
* Tăng cường an toàn (hardening) cho các hệ thống điều hành.
* Quản lý cấu hình của từng máy.
* Xây dựng bộ quy định quản lý hệ thống mạng nội bộ nhằm quản lý các thành phần trên.
* Xây dựng các tiêu chuẩn và quy trình thao tác trên mạng nội bộ.
* Đội ngũ cán bộ kỹ thuật có trình độ, chuyên nghiệp và có kinh nghiêm bảo mật.
* Hạ tầng kỹ thuật bảo mật được đổi mới và cập nhật thường xuyên, hiệu quả bảo mật

Cơ chế bảo mật.

Các mức bảo mật gồm:

* Bảo mật mức Hệ thống
* Bảo mật mức ứng dụng
* Bảo mật thiết bị đường truyền
* Bảo mật đối với người sử dụng
1. Bảo mật mức hệ thống:

Sử dụng cơ chế bảo mật của Hệ điều hành: Áp dụng các cơ chế bảo mật sẵn có trên hệ điều hành (WINDOW, UNIX). Tất cả  các hệ điều hành đều có mức bảo mật cao, người dùng cần đăng nhập bằng mật khẩu; có cơ chế phân quyền sử dụng rất chặt chẽ;…

Sử dụng cơ chế bảo mật của Hệ quản trị Cơ sở dữ liệu (CSDL): Áp dụng cơ chế bảo mật sẵn có của Hệ quản trị cơ sở dữ liệu SQL. Trong hệ CSDL, người quản trị hệ thống có thể gán cho người sử dụng quyền truy nhập tới mức đối tượng và với mỗi một đối tượng lại có thể gán các quyền khác nhau. Ví dụ một người có thể sử dụng câu lệnh truy vấn (SELECT),bổ sung (INSERT), cập nhật (UPDATE), loại bỏ (DELETE) khi người quản trị gán quyền sử dụng hoặc không cho phép sử dụng các lệnh trên.

1. Bảo mật Mức ứng dụng

Các biện pháp xây dựng mức bảo mật ứng dụng bằng cách xây dựng các module có các chức năng sau:

-  Phân nhóm, cấp phát User; Cấp phát quyền; Cấp phát vùng tài nguyên

* Theo dõi truy cập
* Định danh và xác thực người dùng
* Giới hạn thời hạn
1. Bảo mật thiết bị và đường truyền

Sử dụng các thiết bị phần cứng làm tường lửa để phục vụ việc bảo mật hệ thống như: Máy chủ; Thiết bị chuyên dụng Firewall của một số hang Cisco, Microsoft, Fortinet…

1. Bảo mật đối với người sử dụng

Vấn đề bảo mật đối với người sử dụng đặt ra là khá cần thiết. Để hạn chế được các nguy cơ mất an toàn trên, [.................](http://trangco.vn) đã xây dựng các quy chế cụ thể như sau: Xây dựng các  quy định cụ thể cho từng phân ban trong đơn vị; Xây dựng quy chế về phân quyền truy cập và khuyến cáo sử dụng thông tin chặt chẽ trong mạng đối với các đối tượng sử dụng.

Sao lưu và khôi phục dữ liệu

1. An toàn dữ liệu

Các giải pháp an toàn dữ liệu:

* Sử dụng hệ phòng chống cháy nổ, chống sét, nguồn điện sẵn có
* Sử dụng ổn áp LIOA để giảm hiện tượng/ giảm của nguồn điện
* Dùng USP để tránh mất điện đột ngột
* Dữ liệu được sao lưu thường xuyên
1. Sao lưu và khôi phục dữ liệu:
* Các phương thức sao lưu phổ biến:
* Full backup: Là phương pháp sao lưu toàn bộ, dùng để sao lưu tất cả các thông tin được chọn, không quan tâm đến thông tin đó được cập nhật vào thời điểm nào và các lần sao lưu trước đó. Phương pháp này cho phép sao lưu đầy đủ nhất, nhưng tốn kém về thời gian và phương tiện sao thông
* Incremental Backup: Là phương pháp sao lưu gia tăng, dùng để sao lưu tất cả cá thông tin được chọn mà có sự thay đổi hoặc cập nhật so với lần sao lưu trước đó. Phương thức này cho phép tiết kiệm tối đa thời gian và chi phí thiết bị sao lưu.
* Differential Backup: Là phương thức sao lưu khác biệt. Dùng để sao lưu tất cả các thông tin được chọn mà có sự thay đổi hoặc cập nhật so với lần sao lưu đầy đủ (full backup) trước đó.
* Chiến lược sao lưu, khôi phục:

Chiến lược sao lưu, khôi phục được thiết lập do người quản lý công việc sao lưu và được hỗ trợ bằng những tiện ích phần mềm có sẵn hoặc được xây dựng. Việc hoạch định chiến lược sao lưu tối ưu phải phụ thuộc vào qui mô, tầm cỡ của hệ thống và độ quan trọng của dữ liệu và tính chất nghiệp vụ của hệ thống.

Các phương án đảm bảo an toàn hệ thống:

* Phương án bảo đảm an toàn cháy nổ:
* Trung tâm phát tín hiệu được trang bị hệ thống phòng cháy và chữa cháy.
* Nghiêm cấm để các thiết bị dùng điện, dây điện gần các thiết bị dễ cháy nổ.
* Kiểm tra hệ thống dây dẫn điện và vỏ bọc an toàn của dây định kỳ 1 tháng 1 lần.
* Kiểm tra tiếp điện ở cầu dao định kỳ hàng tuần.
* Hệ thống tiếp địa dành cho nguồn và hệ thống truyền dẫn tín hiệu.
* Nghiêm cấm mọi hành vi tự ý tác động tới hệ thống điện, mọi sự tác động tới hệ thống điện phải có lịch trình và thực hiện theo đúng chức năng nhiệm vụ phòng ban được giao.
* Cán bộ công nhân viên trong công ty có nhiệm vụ báo cáo kịp thời mọi sự cố liên quan tới hệ thống điện cho phòng điều hành để kịp thời xử lý.
* Khi lắp đặt thêm phụ tải phải tính toán, xem xét cụ thể độ chịu tải của hệ thống nói chung và độ ổn định, an toàn của thiết bị. Ngoài ra còn cần xem xét cấu trúc hệ thống điện để bảo đảm sự đồng đều giữa các pha điện.
* Nghiêm cấm mang chất cháy nổ vào trong phòng máy, phòng làm việc trừ trường hợp bắt buộc, khi nạp ga bổ sung cho hệ thống lạnh phải có sự kiểm tra giám sát chặt chẽ của bộ phận trực.
* Nghiêm cấm thắp hương, các hành vi dẫn tới cháy nổ.
* Thường xuyên lau chùi kiểm tra các thiết bị để đảm bảo độ an toàn cháy nổ. Bảo dưỡng định kỳ các thiết bị cũng như hệ thống phòng cháy chữa cháy.
* Đào tạo, tập huấn các nhân viên công ty để đảm bảo ứng phó nhanh trong trường hợp khẩn cấp. Tích cực tuyên truyền, giáo dục ý thức mọi thành viên về công tác phòng cháy chữa cháy.
* Phương án đảm bảo an toàn về kỹ thuật:
* Đảm bảo luôn có trang thiết bị thay thế khi cần thiết
* Đối với truyền dẫn, có luồng quang backup ở trạng thái dự phòng
* Trong hệ thống Trung tâm thu phát tín hiệu, các hệ thống dây cáp, điện, mạng, cáp đồng phải được bố trí trục riêng rẽ và gọn gàng.
* Có sổ nhật ký lỗi và các phương án khắc phục sự cố.
* Có chu trình đo kiểm chất lượng hệ thống hàng tháng, hàng quý, tổng hợp và rút kinh nghiệm.
* Phương án đảm bảo an toàn khi bị mất điện:
* Toàn bộ thiết bị đặt tại Trung tâm thu phát tín hiệu phải được cung cấp nguồn điện thông qua hệ thống lưu điện UPS chịu tải tối đa 120 phút.
* Chạy máy phát điện khi bị sự cố mất điện lưới
* Báo thông tin cho phụ trách Trung tâm thu phát tín hiệu truyền hình Internet
* Gọi điện thông báo tình trạng cho đơn vị trực tiếp phụ trách nguồn điện
* Viết báo cáo vê trạng thái hệ thống
* Định kỳ đo trạng thái acquy và lên phương án thay thế kịp thời khi có sự cố
* Kiểm tra phối hợp với điện lực và các cơ quan chức năng của quận và thành phố.

Hệ thống kỹ thuật thiết kế đảm bảo khả năng mở rộng khi số lượng người truy cập tăng lên. Hệ thống được dự phòng thông qua việc luôn có hệ thống máy chủ chờ sẵn dạng ngủ đông. Ở chế độ bình thường hệ thống máy sẽ hoạt động ở mức tối thiểu gần như tắt máy. Khi cần thiết hệ thống có thể bật ở chế độ chạy bình thường như các máy chủ khác chỉ trong thời gian rất ngắn từ vài giây đến vài phút tùy vào mức độ ưu tiên khi bật.

Khi cần thiết hệ thống có thể bật ở chế độ chạy ở dạng công nghệ chụp ảnh ổ cứng, giúp cho việc cài đặt mới chỉ diễn ra trong thời gian ngắn như:

* Sắp xếp đĩa cứng và dọn dẹp rác trên Máy chủ định kỳ tuần một lần;
* Thông báo cho người sử dụng trước 24 giờ khi tắt máy chủ để cài đặt lại hoặc nâng cấp sửa chữa;
* Hệ thống không bị ngừng cung cấp dịch vụ quá 60 phút ngay cả khi sửa chữa;
* Đảm bảo giải đáp thắc mắc và hỗ trợ khách hàng 24/24;
	+ Thiết lập cơ chế cảnh báo thành viên khi đăng các thông tin có nội dung vi phạm (bộ lọc).

Mạng xã hội ................. tiến hành thiết lập  hệ thống bộ lọc từ khóa có cơ chế cảnh báo các thành viên khi đăng tải thông tin có nội dung vi phạm thông qua việc hiển thị cảnh báo hoặc gửi tin nhắn nhắc nhở thành viên.. Đồng thời các từ khóa xấu, không phù hợp sẽ tự động nhận diện các từ khóa nhạy cảm và thay thế bằng các ký tự được định nghĩa có sắn và  khi hiển thị được thay thế thành “\*\*\*\*\*\*\*\*”. Bộ lọc từ hiện nay gồm những từ: Chống lại Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội; phá hoại khối đại đoàn kết dân tộc; tuyên truyền chiến tranh, khủng bố; gây hận thù, mâu thuẫn giữa các dân tộc, sắc tộc, tôn giáo; Tuyên truyền, kích động bạo lực, dâm ô, đồi trụy, tội ác, tệ nạn xã hội, mê tín dị đoan, phá hoại thuần phong, mỹ tục của dân tộc; Tiết lộ bí mật nhà nước, bí mật quân sự, an ninh, kinh tế, đối ngoại và những bí mật khác do pháp luật quy định; Đưa thông tin xuyên tạc, vu khống, xúc phạm uy tín của tổ chức, danh dự và nhân phẩm của cá nhân; Quảng cáo, tuyên truyền, mua bán hàng hóa, dịch vụ bị cấm; truyền bá tác phẩm báo chí, văn học, nghệ thuật, xuất bản phẩm bị cấm, xuyên tạc, vu khống, nhạo báng, xúc phạm uy tín tới tổ chức, cá nhân….và sẽ bổ sung, cập nhật trong quá trình hoạt động.

* Thiết lập cơ chế “Báo cáo vi phạm”: Thành viên tham gia diễn đàn sử dụng sử dụng một chức năng gọi là “Báo cáo vi phạm” để gửi các báo cáo vi phạm tới hệ thống quản lý của diễn đàn để Ban Quản trị diễn đàn có công cụ quản lý và xử lý đúng.
* Ngoài ra các thành viên quản trị diễn đàn (nhân sự kiểm duyệt nội dung) còn thường xuyên kiểm tra các nội dung mới đăng, nhằm phát hiện các nội dung vi phạm nhưng được đăng tải một các khéo léo hoặc chưa có tiền lệ.
* Xử lý vi phạm: Tùy từng hành vi, nội dung vi phạm của thành viên mà ban quản trị sẽ có những hình thức xử phạt tương ứng. Quy chế xử phạt được đăng tải công khai tại trang chủ của .................
* Danh sách từ khóa được xây dựng trên cơ sở các quy định của pháp luật hiện hành bao gồm các từ khóa có nội dung thông tin quy định tại Điều 5 của Nghị định 72 bao gồm: Chống lại Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội; phá hoại khối đại đoàn kết dân tộc; tuyên truyền chiến tranh, khủng bố; gây hận thù, mâu thuẫn giữa các dân tộc, sắc tộc, tôn giáo; Tuyên truyền, kích động bạo lực, dâm ô, đồi trụy, tội ác, tệ nạn xã hội, mê tín dị đoan, phá hoại thuần phong, mỹ tục của dân tộc; Tiết lộ bí mật nhà nước, bí mật quân sự, an ninh, kinh tế, đối ngoại và những bí mật khác do pháp luật quy định; Đưa thông tin xuyên tạc, vu khống, xúc phạm uy tín của tổ chức, danh dự và nhân phẩm của cá nhân; Quảng cáo, tuyên truyền, mua bán hàng hóa, dịch vụ bị cấm; truyền bá tác phẩm báo chí, văn học, nghệ thuật, xuất bản phẩm bị cấm;Danh sách từ khóa được cập nhật thường xuyên

Mạng xã hội .................  sẽ tiến hành việc giám sát cũng như cảnh báo việc người dùng đăng các nội dung vi phạm lên website bằng các biện pháp cụ thể như sau:

+ Bất kì nội dung nào người sử dụng muốn đưa lên website đều phải trải qua khâu kiểm duyệt của ban quản trị để đảm bảo không có bất kì nội dung trái với quy định sử dụng mạng xã hội và trái với các quy định của pháp luật được đưa lên

+ Nhằm đảm bảo an toàn cho hệ thống và hiệu quả vận hành các thành viên Ban quản trị Mạng xã hội ................. sẽ thường xuyên kiểm tra, giám lưu lượng truy cập vào các nội dung được người sử dụng đưa lên. Thông qua hình thức này các nội dung có lượng truy cập tăng cao đột biến tại một thời điểm sẽ được các thành viên vận hành hệ thống website kiểm tra và đánh giá sơ bộ. Nếu có đánh giá sơ bộ nội dung đó là vi phạm ngay lập tức bộ phận vận hành hệ thống sẽ thông báo trực tiếp đến đội ngũ quản trị viên để tiến hành loại bỏ ngay lập tức nội dung vi phạm. Công việc theo dõi này được tiến hành liên tuc.

Sau khi từ chối đăng tải, gỡ bỏ nội dung vi phạm của người sử dụng tùy vào mức độ vi phạm, Mạng xã hội .................  sẽ quyết định các hình thức xử lý như sau:

+ Tất cả những người sử dụng sẽ nhận được email thông báo từ chối hoặc gỡ bỏ nội dung mà người sử dụng mong muốn đăng tải hoặc đã đăng tải trên Mạng xã hội ................. . Đồng thời đưa thành viên vi phạm vào danh sách theo dõi của website

+ Ngoài ra, tùy vào mức độ vi phạm, ban quản trị Mạng xã hội .................  sẽ tiến hành các biện pháp xử phạt với người sử dụng vi phạm: như Ban quản trị sẽ tiến hành khóa chức năng đăng tin trong thời hạn 30 ngày,  tạm khóa tài khoản trong vòng 30 ngày, hoặc khóa tài khoản vĩnh viễn..

Đội ngũ nhân viên kiểm tra nội dung sẽ rà soát thông tin ở các mục một cách ngẫu nhiên và định kỳ để phát hiện và loại bỏ các thông tin xấu.

Hệ thống  tự phân tích dữ liệu người dùng đăng tải lên website thông qua việc phân tích dữ liệu gửi lên dưới dạng các mã HTML và so sánh với kho dữ liệu xấu được tích lũy từng ngày, nếu có dữ liệu trùng với dữ liệu xấu, hệ thống sẽ thông báo để ban quản trị biết và kiểm duyệt lại nội dung.

* Sẵn sàng kết nối, xác thực thông tin các nhân với cơ sở dữ liệu về chứng minh nhân dân hoặc hệ thống mã số cá nhân quốc gia theo yêu cầu của cơ quan có thẩm quyền.

.................  sẵn sàng kết nối, xác thực thông tin cá nhân với cơ sở dữ liệu điện tử về chứng minh nhân dân hoặc hệ thống mã số cá nhân quốc gia theo yêu cầu của cơ quan có thẩm quyền: Hệ thống có những chức năng kết xuất thông tin cá nhân người dùng từ cơ sở dữ liệu dưới dạng .xls theo các giao thức trao đổi và tích hợp dữ liệu trực tiếp như FTP hoặc theo các giao thức gián tiếp qua email như SMTP. Các chức năng này sẵn sàng kết nối, xác thực thông tin cá nhân với cơ sở dữ liệu điện tử về chứng minh nhân dân hoặc hệ thống mã số cá nhân quốc gia theo yêu cầu của cơ quan có thẩm quyền.

* Thực hiện đăng ký, lưu trữ thông tin cá nhân của thành viên:

Để trở thành thành viên tham gia vào Mạng xã hội .................  người sử dụng bắt buộc phải thực hiện việc đăng ký để trở thành thành viên. Việc đó đồng nghĩa rằng, người sử dụng đồng ý với các điều khoản và điều kiện gia nhập do  đưa ra và việc cung cấp các thông tin cá nhân một cách chính xác và đầy đủ là một điều kiện bắt buộc và là bước đầu tiên. Thông tin cá nhân bao gồm:

Họ và tên;

Ngày, tháng, năm sinh;

Số chứng minh nhân dân hoặc số hộ chiếu, ngày cấp, nơi cấp;

Số điện thoại, địa chỉ email.

Lưu ý: Để sử dụng mạng xã .................   bạn phải từ 14 tuổi trở lên và tiến hành đăng ký thành viên. Nếu bạn dưới 14 tuổi và chưa có hộ chiếu, người giám hộ hợp pháp của bạn  sẽ quyết định việc đăng ký thông tin cá nhân của mình để thể hiện sự cho phép bạn trở thành thành viên của ................. và người giám hộ đó chịu trách nhiệm trước pháp luật về việc đăng ký đó. Để đăng ký thành viên bạn phải chứng thực rằng bạn đủ 14 tuổi hoặc lớn hơn bằng cách nhập vào năm sinh chính xác của mình và tự chịu trách nhiệm về những thông tin mà bạn khai báo khi đăng ký cũng như những thông tin bạn đăng tải khi đã trở thành thành viên của.................

Trẻ dưới 14 tuổi hoặc độ tuổi tối thiểu tương đương theo quy định pháp luật có liên quan, không được phép tạo tài khoản của riêng mình, trừ khi cha mẹ của trẻ đã đồng ý thông qua toàn bộ hoặc là một phần của quy trình tạo tài khoản cho trẻ em.

Nếu bất kỳ lúc nào cha mẹ cần truy cập, sửa hoặc xóa dữ liệu liên kết với tài khoản của họ hoặc tài khoản của con họ, thì có thể liên hệ với chúng tôi thông qua Hotline hoặc Email.

5.2.9. Xác thực người sử dụng dịch vụ thông qua tin nhắn gửi đến số điện thoại hoặc đến hộp thư điện tử khi đăng ký sử dụng dịch vụ hoặc thay đổi thông tin cá nhân.

Người sử dụng sau khi tìm hiểu và đồng ý với các điều khoản do Mạng xã hội ................. đưa ra và cung cấp đúng, đầy đủ thông tin theo yêu cầu của Ban quản trị Mạng xã hội [.................](http://trangco.vn) sẽ tiến hành xác thực  thông tin người sử dụng qua email bằng cách: hệ thống sẽ tự động gửi vào hòm thư điện tử của người sử dụng một đường link xác nhận thông tin. Người sử dụng sẽ tiến hành kích hoạt tài khoản của mình bằng cách click vào đường link được gửi đến Email của mình.

Ngoài ra, Mạng xã hội ................. sẽ áp dụng phương pháp kích hoạt tài khoản sử dụng thông qua tin nhắn gửi đến số điện thoại được người sử dụng cung cấp và đăng ký nhận tin tại Mạng xã hội http .................. Sau khi người sử dụng đồng ý với các điều khoản, hệ thống sẽ tự động gửi mã xác nhận vào số điện thoại được đăng ký và yêu cầu người sử dụng xác nhận và việc đăng ký thành viên được hoàn tất.

5.2.10. Ngăn chặn hoặc loại bỏ thông tin vi phạm các quy định tại Điều 5 Nghị định số 72/2013/NĐ-CP khi có yêu cầu từ cơ quan quản lý nhà nước có  thẩm quyền;

Ngay khi có yêu cầu loại bỏ thông tin vi phạm từ cơ quan nhà nước có thẩm quyền, người chịu trách nhiệm quản lý nội dung thông tin và phòng nội dung sẽ tích cực hợp tác và rà soát để xác định nội dung vi phạm này. Tất cả quy trình rà soát sẽ diễn ra nhanh chóng và chậm nhất trong vòng 3 giờ kể từ khi có yêu cầu, nội dung vi phạm sẽ bị loại bỏ khỏi Mạng xã hội ..................

Cơ quan nhà nước có yêu cầu loại bỏ bài viết có nội dung vi phạm sẽ liên hệ trực tiếp với người kiểm duyệt nội dung theo thông tin dưới đây:

 Họ và tên: Nguyễn Hoàng Long

 Chức vụ:  Phó giám đốc

 Điện thoại: 0914 318393

 Email: tonydo@live.com

Quy trình loại bỏ nội dung vi phạm theo khoản 1 Điều 5 Nghị định 72/2013/NĐ-CP:

* Bước 1: Tiếp nhận được thông tin về nội dung vi phạm từ người sử dụng, cơ quan nhà nước có thẩm quyền (qua email, điện thoại, văn bản, báo cáo vi phạm)
* Bước 2: Nhân viên tiếp nhận thông tin chuyển thông tin tới người quản lý nội dung
* Bước 3: Người quản lý nội dung xác định nội dung vi phạm thuộc chuyên mục nào, người phụ trách trực tiếp chuyên mục, làm việc với cá nhân viên quản lý trực tiếp chuyên mục
* Bước 4: Nhân viên quản lý trực tiếp chuyên mục tiến hành gỡ bỏ nội dung vi phạm khỏi chuyên mục
* Bước 5: Nhân viên quản lý trực tiếp chuyên mục làm việc với bộ phận kĩ thuật tiến hành chặn tài khoản người sử dụng vi phạm, đồng thời sẵn sàng cung cấp thông tin người sử dụng vi phạm cho cơ quan nhà nước có thẩm quyền khi được yêu cầu
* Bước 6: Họp rút kinh nghiệm, kiểm điểm các nhân sự để lọt nội dung

Tất cả các bước trong quy trình gỡ bỏ nộ dung vi phạm sẽ được tiến hành trong vòng 03 giờ kể từ khi nhận được thông tin cảnh báo.

* Hệ thống Máy chủ website .................
* Hệ thống ................. được đặt máy chủ tại Việt Nam: nhằm đáp ứng việc thanh tra, kiểm tra, lưu trữ, cung cấp thông tin theo yêu cầu của cơ quan quản lý nhà nước có thẩm quyền và giải quyết khiếu nại của khách hàng đối với việc cung cấp dịch vụ theo quy định.

        Địa chỉ đặt máy chủ: Công ty dữ liệu VNPT – Chi nhánh Tổng công ty dịch vụ viễn thông

Địa chỉ : Nhà Internet, Lô 2A Làng Quốc Tế Thăng Long, Cầu Giấy, Hà Nội
Điện thoại: 043 793 0514                                          Hotline: 0945 451 599
- Cách thức vận hành hệ thống máy chủ:

**6.3. Phương án tài chính nhằm bảo đảm hoạt động của mạng xã hội:**

**6.3.1. Nguồn đầu tư:**

- Từ nguồn vốn của Công ty: 100,000,000 đồng

- Từ hoạt động dịch vụ khác như: Dịch vụ viễn thông, các dịch vụ giá trị gia tăng trên mạng do công ty cung cấp, dự kiến: 1,000,000,000 đồng/năm.

Hoạt động quản lý thông tin:

a) Xây dựng và thực hiện thỏa thuận cung cấp và sử dụng dịch vụ mạng xã hội phù hợp theo các quy định tại Nghị định số .../...../NĐ-CP và được đăng tải trên trang chủ của http://trangco. (theo bản Bản thỏa thuận đính kèm)

Cam kết có hiệu lực từ ngày Mạng xã hội .................  chính thức đi vào hoạt động, tất cả thành viên, cá nhân, tổ chức sử dụng dịch vụ tại Mạng xã hội .................  bắt buộc phải đọc và cam kết nội dung này khi đăng ký và sử dụng dịch vụ của Mạng xã hội  Cam kết này ....... có giá trị pháp lý là một văn bản giao kết giữa Mạng xã hội ................. và người sử dụng, tất cả thành viên sử dụng bất kỳ dịch vụ nào trên mạng xã hội này được hiểu là mặc định đã ký vào cam kết này và chịu trách nhiệm trước pháp luật nước Việt Nam.

b) Bảo đảm người sử dụng phải đồng ý thỏa thuận sử dụng dịch vụ mạng xã hội bằng phương thức trực tuyến thì mới có thể sử dụng được các dịch vụ, tiện ích của mạng xã hội;

Để nhận được sự hỗ trợ từ mạng xã hội Mạng xã hội .................  người sử dụng cần phải hiểu và đồng ý với quy chế quản lý của Mạng xã hội ................., tài khoản của bạn phải đăng ký đầy đủ các thông tin trung thực, chính xác. Nếu có sự thay đổi, bổ sung về thông tin, bạn cập nhật ngay cho chúng tôi theo hướng dẫn được quy định trên website Mạng xã hội................. . Bạn đảm bảo rằng, thông tin hiện trạng của bạn là mới nhất, đầy đủ, trung thực và chính xác và bạn phải chịu trách nhiệm toàn bộ các thông tin bạn cung cấp.

Bạn có trách nhiệm bảo mật thông tin tài khoản bao gồm: Mật khẩu, số điện thoại bảo vệ tài khoản, giấy tờ tùy thân, Email bảo vệ tài khoản và mật khẩu. Nếu những thông tin trên bị tiết lộ dưới bất kỳ hình thức nào thì bạn phải chấp nhận những rủi ro phát sinh. Mạng xã hội .................  sẽ căn cứ vào những thông tin hiện có trong tài khoản để làm căn cứ quyết định chủ sở hữu tài khoản nếu có tranh chấp và Mạng xã hội.................  sẽ không chịu trách nhiệm về mọi tổn thất phát sinh. Thông tin Giấy tờ tùy thân đăng ký trong tài khoản là thông tin quan trọng nhất để chứng minh chủ sở hữu tài khoản.

Bạn đồng ý sẽ thông báo ngay cho mạng xã hội Mạng xã hội ..... về bất kỳ trường hợp nào sử dụng trái phép tài khoản và mật khẩu của bạn hoặc bất kỳ các hành động phá vỡ hệ thống bảo mật nào. Bạn cũng bảo đảm rằng, bạn luôn thoát tài khoản của mình sau mỗi lần sử dụng.

Mạng xã hội .................  quan tâm tới sự an toàn và riêng tư của tất cả thành viên đăng ký tài khoản và sử dụng sản phẩm của mình, đặc biệt là trẻ em. Vì vậy, nếu bạn là cha mẹ hoặc người giám hộ hợp pháp, bạn có trách nhiệm xác định xem sản phẩm, nội dung nào Mạng xã hội .................  thích hợp cho con của bạn. Tương tự, nếu bạn là trẻ em thì phải hỏi ý kiến cha mẹ hoặc người giám hộ hợp pháp của bạn xem sản phẩm, nội dung mà bạn sử dụng có phù hợp với bạn không.

Khi phát hiện ra lỗi của sản phẩm , các vấn đề gây ảnh hưởng tới hoạt động bình thường của Mạng xã hội ................. cũng như các sản phẩm liên quan, bạn hãy thông báo cho chúng tôi qua đường email: ……………………. hoặc đường dây nóng ………………

Bạn cam kết thực hiện trách nhiệm bảo đảm sử dụng hợp pháp nội dung thông tin số đưa lên đăng tải trên hệ thống mạng Internet và mạng viễn thông.

Bạn có thể sẽ bị xử phạt vi phạm hành chính, bị truy tố trách nhiệm hình sự nếu bạn vi phạm về quyền tác giả, quyền liên quan khi bạn sử dụng mạng xã hội trực tuyến của Mạng xã hội................. .

Bạn phải tuân thủ tuyệt đối thỏa thuận này về các hành vi cấm. Nếu vi phạm một hoặc nhiều hành vi, tùy thuộc vào mức độ vi phạm Mạng xã hội .................  sẽ khóa tài khoản vĩnh viễn, tước bỏ mọi quyền lợi của bạn đối các sản phẩm của Mạng xã hội ................. và sẽ yêu cầu cơ quan chức năng can thiệp nếu cần thiết..

c) Cơ chế phối hợp để loại bỏ nội dung vi phạm sau 03 (ba) giờ kể từ khi tự phát hiện hoặc có yêu cầu của cơ quan nhà nước có thẩm quyền (bằng văn bản, điện thoại, email)

Để tạo một môi trường lành mạnh trên mạng xã hội ................. , các thông tin lưu trữ, đăng tải, chia sẻ, trao đổi trên website đều được kiểm duyệt 1 cách chặt chẽ nhằm đảm bảo tính xác thực, nội dung của các thông tin đăng tải, chia sẻ, trao đổi không vi phạm điều cấm của pháp luật về quản lý, sử dụng thông tin trên mạng internet. Nội dung kiểm duyệt: Bao gồm nội dung, hình ảnh và âm thanh, được thể hiện dưới dạng: Text (chữ), image (hình ảnh) và video (âm thanh), Thông qua hình thức kiểm duyệt bằng hệ thống phần mềm tự động kiểm duyệt và bằng đội ngũ nhân sự, mạng xã hội .................  sẽ thiết lập cơ chế cảnh báo thành viên khi đăng các thông tin vi phạm.

Khi phát hiện, hoặc khi có yêu cầu của cơ quan nhà nước có thẩm quyền hoặc nghi ngờ có các nội dung vi phạm này, hệ thống sẽ tự động chuyển các nội dung vi phạm sang dạng cảnh báo và chờ xử lý. Trong vòng 3 (ba) giờ, bộ phận kiểm duyệt nội dung của Mạng xã hội ................. sẽ trực tiếp kiểm tra lại các cảnh báo này và quyết định việc xóa bỏ hay cho phép hiển thị các nội dung này trên website, đồng thời sẽ cảnh báo vi phạm đến người sử dụng (thành viên đăng tải thông tin) và có thể khóa tài khoản vi phạm vĩnh viễn.

Quy trình kiểm duyệt:

+ Kiểm duyệt lần một (kiểm duyệt bằng hệ thống kỹ thuật, triển khai bộ lọc nội dung)

* Kiểm duyệt nội dung thông tin thông qua bộ lọc từ khóa nhằm ngăn chặn những nội dung xấu: Danh sách từ khóa được xây dựng trên cơ sở các quy định của pháp luật hiện hành bao gồm các từ khóa có nội dung thông tin quy định tại Điều 5 của Nghị định 72 bao gồm : Chống lại Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội; phá hoại khối đại đoàn kết dân tộc; tuyên truyền chiến tranh, khủng bố; gây hận thù, mâu thuẫn giữa các dân tộc, sắc tộc, tôn giáo; Tuyên truyền, kích động bạo lực, dâm ô, đồi trụy, tội ác, tệ nạn xã hội, mê tín dị đoan, phá hoại thuần phong, mỹ tục của dân tộc; Tiết lộ bí mật nhà nước, bí mật quân sự, an ninh, kinh tế, đối ngoại và những bí mật khác do pháp luật quy định; Đưa thông tin xuyên tạc, vu khống, xúc phạm uy tín của tổ chức, danh dự và nhân phẩm của cá nhân; Quảng cáo, tuyên truyền, mua bán hàng hóa, dịch vụ bị cấm; truyền bá tác phẩm báo chí, văn học, nghệ thuật, xuất bản phẩm bị cấm;
* Danh sách từ khóa được cập nhật thường xuyên. Khi phát hiện hoặc nghi ngờ có các nội dung vi phạm này, hệ thống sẽ tự động chuyển các nội dung vi phạm sang dạng cảnh báo và chờ xử lý. Bộ phận kiểm duyệt nội dung của Mạng xã hội ................. sẽ trực tiếp kiểm tra lại các cảnh báo này và quyết định việc xóa bỏ hay cho phép hiển thị các nội dung này trên website.
* Kiểm duyệt nội dung thông tin thông qua việc hạn chế các nguồn thông tin có nội dung vi phạm: Khi Thành viên sử dụng chức năng chia sẻ nguồn thông tin cho cộng đồng, hệ thống sẽ tự động lưu lại toàn bộ các nguồn thông tin này. Bộ phận kiểm duyệt nội dung sẽ thực hiện việc xem xét các nội dung của nguồn, trường hợp các nội dung này không phù hợp, hệ thống sẽ bổ sung nguồn vào danh sách các từ khóa nhằm ngăn chặn tối đa việc đăng tải các nội dung vi phạm, đồng thời thực hiện việc gỡ bỏ nguồn khỏi hiện thị của diễn đàn

+  Kiểm duyệt lần hai (kiểm duyệt bằng đội ngũ nhân sự),

* Đội ngũ nhân sự điều hành Mạng xã hội ................. là những người có kiến thức chuyên môn cao, giàu kinh nghiệm, nắm vững các quy định của pháp luật hiện hành về quản lý, cung cấp, sử dụng thông tin trên trang thông tin điện tử tổng hợp và mạng xã hội. Mạng xã hội thực hiện việc kiểm duyệt 24/7 nhằm kịp thời phát hiện và loại bỏ các nội dung vi phạm;
* Hàng ngày, đội ngũ nhân sự sẽ thực hiện việc kiểm duyệt thông tin trong danh sách cảnh báo do hệ thống cập nhật. Những nội dung vi phạm sẽ xóa bỏ ngay lập tức. Đồng thời, tùy mức độ vi phạm, Ban Quản trị Mạng xã hội ................. sẽ quyết định khóa tạm thời hoặc khóa vĩnh viễn tài khoản của Thành viên khi Thành viên đó có hành vi vi phạm;
* Mạng xã hội ................. còn thực hiện việc kiểm duyệt thông tin thông qua thông chức năng “Báo cáo vi phạm” và “Tiếp nhận và xử lý cảnh báo thông tin vi phạm từ người sử dụng” của các Thành viên khác. Khi nhận được thông báo, đội ngũ nhân sự có nhiệm vụ xác nhận lại các thông tin này, nếu phát hiện vi phạm sẽ xử lý theo quy trình chung;
* Việc kiểm duyệt được thực hiện hằng ngày, những thông tin vi phạm cũng có thể loại bỏ ngay nội dung vi phạm chậm nhất sau 03 giờ kể từ khi tự phát hiện hoặc có yêu cầu của Cơ quan Nhà nước có thẩm quyền (bằng văn bản, email, điện thoại)
* Trường hợp quý cơ quan quản lý, người sử dụng hoặc người tham gia phát hiện các nội dung được chia sẻ trên Mạng xã hội ................. có dấu hiệu vi phạm có thể phản ánh và gửi thông tin cho Ban quản trị theo các cách sau:

1) Gửi đường link vi phạm về địa chỉ email:

2) Gọi điện thoại tới số điện thoại trong giờ hành chính để thông báo về vi phạm:

Cố định :                                                         Di động :

Ngoài ra, tất cả các thông tin được thực hiện truyền tải trên Mạng xã hội .................  đều trải qua một giai đoạn kiểm tra về mặt nội dung như kiểm tra chính tả tự động; đảm bảo sự tương thích của nội dung và trình duyệt; đưa các thông tin giúp theo dõi và cập nhật trang (ngày sửa đổi gần nhất, thông tin về phần mềm dùng để mở và xem) và xác định và xử lý các liên kết bị đứt trên website. Sau đó mới được đăng tải trên website và lưu trữ tại máy chủ của công ty.

 Hệ thống kiểm duyệt và quản lý nội dung website

+  Kiểm duyệt nội dung dạng text (chữ): Ban Quản trị Mạng xã hội ................. xây dựng danh sách các từ khóa xấu, không hợp lệ (bad keywords) và có mức độ (thang điểm) của những từ khóa không hợp lệ (bad keywords này) dùng để đánh giá nội dung. Nếu nội dung do Thành viên đưa lên mà trong đó có những từ nằm trong danh sách từ không hợp lệ (bad keywords) và tùy theo số lượng từ xấu xuất hiện mà hệ thống sẽ tự đánh giá xem bài viết đó có hợp lệ hay không. Nếu những bài viết mà hệ thống cho là không phù hợp thì sẽ lưu vào danh sách các bài viết không hợp lệ thì bộ phận kiểm duyệt sẽ dễ dàng hơn trong việc duyệt nội dung.

+ Kiểm duyệt nội dung dạng image (hình ảnh): Khi Thành viên đăng tải hình ảnh tại Mạng xã hội .................   thì các hình ảnh này được Hệ thống tự động lưu vào khu vực lưu trữ riêng. Sau đó những ảnh này sẽ được gửi đến hệ thống phân tích và phân loại theo từ khóa. Những hình ảnh có nội dung vi phạm sẽ được chuyển sang danh sách cảnh báo và chờ xử lý. Bộ phận kiểm duyệt sẽ vào danh sách này xem xét và kiểm duyệt lại lần nữa, nếu đúng ảnh này có nội dung vi phạm thì hệ thống sẽ không duyệt ảnh hoặc xóa ảnh này khỏi hệ thống lưu trữ.

+ Kiểm duyệt nội dung dạng âm thanh (video): Đối với dạng này Mạng xã hội ................. sẽ ưu tiên kiểm duyệt bằng nhân sự một cách trực tiếp. Ban Quản trị phải trực tiếp kiểm duyệt từng video, đảm bảo tính pháp lý và phù hợp với nội dung, quy định

Cơ chế xử lý đối với nội dung sai phạm

* Nhắc nhở, cảnh cáo: Đối với hành vi vi phạm quy định của ................. về thể thức, vị trí; nội dung rác, nội dung quảng cáo, nội dung ảnh hưởng đến uy tín của cá nhân, tổ chức khác có hành vi khác xâm phạm  quyền và lợi ích của ................. Ban Quản trị có quyền xóa, chuyển chuyên mục, lọc bỏ nội dung quảng cáo, thay từ ngữ không phù hợp, tạm ngừng hiển thị chờ kiểm duyệt tùy theo mức độ vi phạm. Đồng thời, Thành viên đó sẽ bị nhắc nhở, cảnh cáo (vi phạm lần đầu) hoặc bị áp dụng hình thức khóa tài khoản tạm thời (07) ngày hoặc khóa tài khoản vĩnh viễn (vi phạm lần thứ ba);
* Khóa tài khoản: Đối với hành vi vi phạm quy định pháp luật về nội dung cấm đăng tải, chia sẻ, trao đổi trên mạng xã hội: Ban Quản trị .................  có quyền khóa, xóa ngay lập tức bài đăng mà không cần thông báo. Đồng thời, Thành viên đó sẽ bị nhắc nhở, cảnh cáo (vi phạm lần đầu) hoặc khóa tài khoản vĩnh viễn (vi phạm lần thứ hai hoặc lần thứ ba);

Ngay khi tự phát hiện hoặc có yêu cầu từ phía cơ quan Nhà nước có thẩm quyền (bằng văn bản, điện thoại, email), nội dung vi phạm sẽ bị loại bỏ trong thời gian tối đa 03 (ba) giờ. Theo cơ chế sau:

* Trường hợp ................. tự phát hiện ra vi phạm
	+ Bước 1: Bộ phần Quản lý nội dung thông tin sễ đánh giá nội dung vi phạm về tính chất và mức độ vi phạm.
	+ Bước 2: Loại bỏ vĩnh viễn nội dung vi phạm khỏi .................
	+ Bước 3: Đưa ra cảnh báo, nhắc nhở về việc không được tái diễn hành vi vi phạm đến tài khoản đăng thông tin vi phạm.
* Trường hợp có yêu cầu từ phía cơ quan Nhà nước có thẩm quyền:
	+ Bước 1: Xác thực thông tin vi phạm
	+ Bước 2: Loại bỏ vĩnh viễn nội dung vi phạm khỏi ....
	+ Bước 3: Đưa ra cảnh báo, nhắc nhở về việc không được tái diễn hành vi vi phạm đến tài khoản đăng thông tin vi phạm.

Các cơ quan nhà nước có thẩm quyền có yêu cầu gửi đến bằng văn bản thì yêu cầu này sẽ được chuyển đến cho trưởng nhóm. Trưởng nhóm xem xét đề nghị và yêu cầu quản trị viên gỡ bỏ thông tin vi phạm theo yêu cầu chậm nhất sau 03 giờ kể từ khi nhận được thông báo.

d) Có biện pháp bảo vệ bí mật thông tin riêng, thông tin cá nhân của người sử dụng;

- Để trở thành thành viên của Mạng xã hội .................,, người sử dụng phải cung cấp đầy đủ các thông tin về: Họ và tên, ngày tháng năm sinh, số chứng minh nhân dân hoặc hộ chiếu, số điện thoại, địa chỉ email... Tất các các thông tin cá nhân nêu trên của các thành viên sẽ được lưu trữ tối thiểu 02 (hai) năm đối với các thông tin về tài khoản, thời gian đăng nhập, đăng xuất, địa chỉ IP của người sử dụng và nhật ký xử lý thông tin được đăng tải; Chúng tôi cam kết  bảo vệ tối đa các thông tin các nhân, sự riêng tư của người sử dụng. Bảo mật thông tin là hình thức chúng tôi thu thập và xử lý các thông tin cá nhân khi người sử dụng Mạng xã hội ................. . Với việc đồng ý chính sách bảo mật thông tin cùng Thỏa thuận thành viên, bạn mặc nhiên chấp nhận cách thức chúng tôi thu thập, lưu trữ, sử dụng, tiết lộ thông tin cá nhân của bạn v.v.. được nêu trong chính sách này.

  Ngoài ra, đề đảm bảo quyền riêng tư tuyệt đối của thành viên về tài khoản cá nhân trên Mạng xã hộ................. , khi đăng ký thành viên hoặc thay đổi thông tin cá nhân hệ thống quản lý và điều hành Mạng xã hội .................  sẽ thực hiện việc xác thực người sử dụng dịch vụ thông qua tin nhắn gửi đến số điện thoại đã đăng ký hoặc đến hộp thư điện tử khi đăng ký sử dụng dịch vụ.

đ) Bảo đảm quyền quyết định của người sử dụng trong việc cho phép thu thập thông tin cá nhân của mình hoặc cung cấp cho tổ chức, doanh nghiệp, cá nhân khác.

- Mạng xã hội.................  đảm bảo quyền quyết định của người sử dụng trong việc cho phép thu thập thông tin cá nhân , tất cả thông tin đều được người sử dụng đồng ý trước khi cung cấp cho Mạng xã hội ................. . Khi đăng kí tài khoản trên Mạng xã hội ................. mặc nhiên người sử dụng đã đồng ý với các thỏa thuận về cung cấp thông tin cá nhân cho Mạng xã hội .................

Ngoài trường hợp cung cấp cho cơ quan chức năng khi có yêu cầu, việc cung cấp thông tin người sử dụng cho bên thứ ba (nếu có) sẽ hoàn toàn do người sử dụng quyết định Mạng xã hội .................  tuyệt đối không tự ý quyết định hay can thiệp vào vấn đề này.

|  |  |
| --- | --- |
|   | **Đại diện theo pháp luật của công ty** |