**PHƯƠNG ÁN KỸ THUẬT CUNGPHIM.COM**

1. **Điều kiện về nhân sự bộ phận kỹ thuật**

* Bộ phận quản lý kỹ thuật tối thiểu có 01 người đáp ứng quy định tại điểm g, điểm h khoản 2 Điều 2 Thông tư số 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(Theo Phụ lục đính kèm)

🡺 Ký hợp đồng lao động với những cá nhân, tổ chức có kinh nghiệm trong lĩnh vực thiết kế và vận hành website

Trong Hợp đồng lao động kèm Quyết định bổ nhiệm sẽ nêu những yêu cầu đối với công việc.

...

...

...

1. **Điều kiện về hệ thống thiết bị kỹ thuật:**

Thiết lập hệ thống thiết bị kỹ thuật có khả năng đáp ứng các yêu cầu sau:

* 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;

**🡺**Dung lượng ổ cứng máy chủ (chính), máy chủ backup, Cơ chế sao lưu dữ liệu?

... Dung lượng ổ cứng: 500Gigabyte – 1Terabyte cho server chính, 500GB server backup.

... Được sao lưu bảng FULL hàng tuần vào ngày thứ 7.

... Chế độ sao lưu: backup toàn bộ database và toàn bộ chương trình lưu ở server cục bộ, sau đó được copy lên cloud bằng chương trình tự động easybackup (chương trình đã đăng ký liciense).

* Tiếp nhận và xử lý cảnh báo thông tin vi phạm từ người sử dụng;

**🡺**Cơ chế nhận thông tin từ user, xử lý, xét duyệt thông tin tự động, thủ công.?

Cơ chế chuyển tải thông báo vi phạm đến user: thời gian, nội dung chuyển tải?

... Tích hợp 2 cơ chế xử lý thông tin:

...1. Tự động: người sử dụng nhập thông tin vào hệ thống, thông tin đó được đi qua bộ lọc được xây dựng trên cơ chế lọc từ khóa gồm: từ khóa nhạy cảm, những từ ảnh hưởng đến thuần phong mỹ tục, từ khóa liên quan đến chính trị.... Khi gập những từ khóa này hệ thống sẽ tự động chuyển thành các ký tự \*\*\* để người khác không đọc được và user này sẽ được hệ thống ghi nhận là bài có nội dung không tốt. Sau đó sẽ được xử lý ở phần 3

...2. Thủ công: người quản trị sẽ tiếp nhận các thông tin qua 1 hệ thống quản trị nội dung. Khi user nhập nội dung xấu, nhạy cảm, spam, bài viết không hợp lệ.... sẽ được admin đánh dấu bằng tay cho hệ thống ghi nhận lại. Sau đó sẽ được xử lý ở phần 3

...3. Cơ chế xử lý thông tin vi phạm: hệ thống đã đếm số lần user vi phạm nội dung, nếu user vi phạm trên 10 lần sẽ được cảnh báo về email và trên giao diện khi vừa đăng nhập vào hệ thống. Nếu user vẫn tiếp tục vi phạm trên 20 lần hệ thống sẽ tự động khóa user đó lại trong 3 ngày không thể đăng vào HT. Sau thời gian này user vẫn tiếp tục vi phạm thêm sẽ bị hệ thống tự động khóa vĩnh viễn.

* Phát hiện, cảnh báo và 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;

**🡺**Các hình thức tấn công, truy cập bất hợp pháp?

Cách thức hoạt động của tường lửa, phần mềm diệt virus?

Phương án ngăn chặn các hoạt động tấn công, truy cập bất hợp pháp?

Mức độ hiệu quả của các phương án trên?

... Các hình thức tấn công phổ biến nhất hiện nay là: tấn công mạng, tấn công từ chối dịch vụ DDOS, tấn công các ứng dụng web, các lỗi liên quan đến bảo mật, lập trình, hoặc do virus tấn công.

... Nhầm giảm bớt các kiểu tấn công này thường các máy chủ sẽ trang bị các tường lửa bằng thiết bị firewall cứng, hay các ứng dụng firewall mềm nhầm chống lại các truy cập trái phép, bảo vệ các nguồn thông tin và sự xâm nhập không mong muốn vào hệ thống. Trên các máy chủ phải trang bị thêm những chương trình diệt virus để phát hiện virus, spyware, keyloger, sniffer.

...

* Có phương án dự phòng bảo đảm duy trì hoạt động an toàn, liên tục và khắc phục khi có sự cố xảy ra, trừ những trường hợp bất khả kháng theo quy định của pháp luật;

**🡺**Máy chủ dự phòng

**...** Máy dự phòng đã được cài toàn bộ chương trình giống máy chủ chính. Khi xảy ra sự cố chỉ cần trỏ domain về địa chỉ ip của máy chủ dự phòng thì hệ thống vẫn hoạt động liên tục.

**...** Trường hợp khi có hỏa hoạn cháy nổ xãy ra thì việc phục hồi sẽ lâu hơn dự kiến.

**...**

* Đảm bảo phải có ít nhất 01 (một) hệ thống máy chủ đặt tại Việt Nam, cho phép tại thời điểm bất kỳ cũng có thể đáp ứng việc thanh tra, kiểm tra, lưu trữ, cung cấp thông tin trên toàn bộ các trang thông tin tiện tử, mạng xã hội do tổ chức, doanh nghiệp sở hữu theo quy định tại 04 điểm (gạch đầu dòng) trên.

**🡺**Ký hợp đồng máy chủ tại Việt Nam

Thực hiện kết nối với cơ quan chức năng khi cần thiết

Cam kết cung cấp đầy đủ và kịp thời khi được cơ quan chức năng yêu cầu

**...**

**...**

**...**

* Thực hiện đăng ký, lưu trữ thông tin cá nhân của thành viên. (Thông tin cá nhân đính kèm tại Phụ lục);

**🡺**Yêu cầu nhập thông tin cá nhân (chủ yếu) khi đăng ký và tùy chọn bổ sung thông tin khác.

Lưu trữ thông tin trên server chính và server dự phòng

... Thông tin người sử dụng đăng ký vào hệ thống sẽ được lưu trữ 5 năm trong cơ sở dữ liệu trên máy chủ chính và máy dự phòng.

... Thông tin đăng ký vào hệ thống bao gồm: Họ và tên, tên đăng nhập, email, mật khẩu.

... Các thông tin phụ: số điện thoại, nơi sinh, giới tính, hình đại diện.... sẽ được tùy chọn cập nhật trong phần settting/profile của hệ thống.

* Thực hiện việc 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.

**🡺**Gửi tin nhắn xác thực qua email. Vd: gửi link xác thực

Cơ chế phản hồi việc xác thực. Vd: thông báo xác nhận thành viên sau khi người dùng click vào đường link đã gửi.

... Khi người sử dụng đăng ký lần đầu tiên, hệ thống sẽ gửi 1 email xác thực tài khoản vào địa chỉ email đã nhập trong phần đăng ký.

... Người dùng cần phải đăng nhập vào email để lấy link xác thực tài khoản, chỉ khi nào người sử dụng click vào link này thì tài khoản mới thực sự được kích hoạt.

... Sau khi hệ thống báo là tài khoản đã được kích hoạt thành công thì lúc này user mới có quyền đăng nhập hệ thống.

... Cơ chế xác thực thứ 2: Nếu người sử dụng không muốn xác thực qua Email thì khi đăng nhập lần đầu tiên vào hệ thống sau khi đăng ký. Hệ thống sẽ cho người sử dụng nhập số điện thoại. Mã code sẽ được gửi đến số điện thoại đó. Người dùng chỉ cần nhập mã code đó vào nơi cần xác thực thì user lập tức được mở.

* 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. (Phụ lục đính kèm);

**🡺**Tạo bộ lọc các từ khóa có nội dung vi phạm

Lập bộ phận xét duyệt nội dung 24/24

Lập đường dây nóng để nhận yêu cầu từ cơ quan quản lý

... Bộ lọc được xây dựng trên cơ chế lọc từ khóa. Khi xuất hiện từ khóa mới không nằm trong bộ lọc thì admin sẽ thêm từ khóa đó vào CSDL để bộ lọc làm việc tốt hơn.

... Ngoài ra còn có bộ phận duyệt tin theo dõi nội dung 24/24. Trường hợp bất khả kháng thì chủ đề đó sẽ tạm thời khóa lại.

... Đường dây nóng phản hồi được đưa lên website trong phần liên hệ.

* Thiết lập cơ chế cảnh báo thành viên khi đăng thông tin có nội dung vi phạm (bộ lọc);

**🡺**Tạo cơ chế cảnh báo tự động

Tạo cơ chế để người dùng tự cảnh báo với nhau

Hình thức cảnh báo: hiển thị thông báo nội dung vi phạm và ngăn chặn, xóa tài khoản khi user đưa tiếp những thông tin vi phạm khác

... Khi người xử dụng tạo nội dung không phù hợp sẽ có cảnh báo được gửi vào email và được đăng tải trong profile cá nhân của người đó.

... Hệ thống sẽ tự động disable user khi tiếp tục vi phạm.

... Ngoài chức năng tự động cảnh báo do hệ thống thì trên giao diện người sử dụng còn có chức năng ”báo cáo vi phạm”. Khi 1 người nào đó bị báo cáo là vi phạm, nội dung này sẽ được gửi về cho admin và người kiểm duyệt sẽ xử lý trường hợp 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 kết nối ngay khi có yêu cầu

Lập đường dây nóng để nhận yêu cầu từ cơ quan quản lý

...

...

...

1. **Điều kiện về quản lý thông tin**

* Có thỏa thuận cung cấp và sử dụng dịch vụ mạng xã hội phù hợp theo các quy định tại Nghị định số 72/2013/NĐ-CP và được đăng tải trên trang chủ của mạng xã hội (nội dung chính của thỏa thuận có tại Phụ lục đính kèm).

**🡺**Hiển thị thỏa thuận cung cấp và sử dụng dịch vụ khi user đăng ký tham gia

Có ô chọn ĐỒNG Ý hoặc KHÔNG ĐỒNG Ý với thỏa thuận trên

* 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;

**🡺**Bảm đảo người dùng phải chọn ĐỒNG Ý mới được phép tham gia

* Có cơ chế phối hợp để có thể loại bỏ ngay nội dung vi phạm khoản 1 Điều 5 Nghị định 72/2013/NĐ-CP**chậm nhất 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). (Nội dung khoản 1 Điều 5 chi tiết theo Phụ lục đính kèm)

**🡺**Lập ban kiểm duyệt nội dung 24/24

Lập đường dây nóng nhận phản hồi, yêu cầu từ cơ quan nhà nước

Thực hiện rà soát tự động, thủ công để tìm kiếm và xử lý nội dung vi phạm.

Thông báo với cơ quan nhà nước sau khi đã xử lý xong (xóa nội dung, chặn user đưa tin, xóa user...)

... Khi xảy ra khiếu nại mà admin không thể giải quyết thì sẽ nhờ đến các cơ quan nhà nước can thiệp. Tài khoản, nội dung của user này sẽ được khóa lại cho đến khi giải quyết xong. Nội dung vi phạm sẽ được admin lọc ra 1 cách dễ dàng để cung cấp cho các cơ quan chức năng.

...

...

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

**🡺**Sẽ có tùy chọn cho user ĐỒNG Ý hoặc KHÔNG ĐỒNG Ý với việc hiển thị, sử dụng thông tin cá nhân

**...**

**...**

**PHỤ LỤC**

1. **YÊU CẦU VỀ KIẾN THỨC CỦA NHÂN SỰ KỸ THUẬT**

*Quy định tại điểm g, điểm h khoản 2 Điều 2 Thông tư số 03/2014/TT-BTTTT ngày 11 tháng 3 năm 2014 của Bộ Thông tin và Truyền thông v/v Quy định chuẩn kỹ năng sử dụng CNTT : Chuẩn kỹ năng sử dụng CNTT nâng cao:*

1. **Điểm g, khoản 2, điều 2, số 03/2014/TT-BTTTT: Mô đun kỹ năng 13 (Mã IU13): Biên tập trang thông tin điện tử (Bảng 07, Phụ lục số 02)**

| **Mã tham chiếu** | **Nội dung/Yêu cầu cần đạt** |
| --- | --- |
| **IU13.1** | **Kiến thức cơ bản về trang thông tin điện tử (website), xuất bản website và các vấn đề liên quan** |
| **IU13.1.1** | **Các khái niệm và thuật ngữ chính** |
| IU13.1.1.1 | 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). |
| IU13.1.1.2 | 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). |
| IU13.1.1.3 | Biết khái niệm giao thức (protocol). Phân biệt các giao thức TCP/IP, HTTP, FTP. |
| **IU13.1.2** | **Xuất bản website** |
| IU13.1.2.1 | 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). |
| IU13.1.2.2 | 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. |
| IU13.1.2.3 | 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. |
| IU13.1.2.4 | 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. |
| IU13.1.2.5 | Hiểu thuật ngữ bản quyền (copyright) đối với các nội dung trên các website. |
| IU13.1.2.6 | Hiểu cần phải tuân thủ các quy định của luật pháp nơi website được đặt đối với việc đăng tải nội dung trên website. |
| **IU13.2** | **Thiết kế website** |
| **IU13.2.1** | **Cơ bản về HTML** |
| IU13.2.1.1 | 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. |
| IU13.2.1.2 | 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>). |
| **IU13.2.2** | **Hoạch định và thiết kế website** |
| IU13.2.2.1 | 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). |
| IU13.2.2.2 | Biết sử dụng các phần mềm ứng dụng làm website. Biết sử dụng phần trợ giúp của phần mềm này. |
| IU13.2.2.3 | 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. |
| IU13.2.2.4 | Biết biên tập tên trang web. |
| IU13.2.2.5 | 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. |
| IU13.2.2.6 | 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). |
| **IU13.3** | **Xây dựng nội dung cho website** |
| **IU13.3.1** | **Văn bản, đoạn, trang** |
| IU13.3.1.1 | Biết cách nhập, biên tập, xóa văn bản. |
| IU13.3.1.2 | Biết các cách định dạng phông chữ như tên, cỡ, đậm, nghiêng, kiểu dáng và màu. |
| IU13.3.1.3 | Biết cách chọn một đoạn, cách đưa vào/loại bỏ các dấu ngắt đoạn, ngắt dòng. |
| IU13.3.1.4 | Biết các cách định dạng đoạn như đặt lề, thụt dòng, đánh số, đánh dấu đầu dòng (bullet). |
| IU13.3.1.5 | Biết cáchđịnh dạng một trang web, cách đặt lề, xử lý màu nền, ảnh nền. |
| **IU13.3.2** | **Siêu liên kết** |
| IU13.3.2.1 | Hiểu khái niệm siêu liên kết (hyperlink), phân biệt siêu liên kết tuyệt đối và tương đối. |
| IU13.3.2.2 | Biết nhập, biên tập và hủy một siêu liên kết thông thường, một siêu liên kết thư điện tử. |
| IU13.3.2.3 | Biết cách xác định đích của siêu liên kết trên cùng cửa sổ, khác cửa sổ. |
| IU13.3.1.4 | Biết cách thay đổi màu siêu liên kết truy cập (visited), không truy cập (unvisited), hoạt động (active). |
| IU13.3.1.5 | Biết khái niệm và cách sử dụng neo (anchor). |
| **IU13.3.3** | **Bảng** |
| IU13.3.3.1 | Biết cách đưa một bảng lên trang web, cách xóa bảng khỏi trang web. |
| IU13.3.3.2 | Biết cách thêm, xóa tiêu đề (caption) của bảng. Biết cách thêm, xóa dòng, cột; thay đổi độ rộng cột, độ cao dòng; hợp, tách các ô của bảng. |
| IU13.3.3.3 | Biết cách căn lề bảng theo lề trái, giữa, phải; cách thay đổi độ rộng biên của bảng; thay đổi các tham số ô. |
| IU13.3.3.4 | Biết cách trang trí bảng: thay đổi màu nền, hình minh họa, ảnh nền của ô và toàn bảng; thêm, loại bỏ đồ họa, ảnh nền của bảng. |
| **IU13.3.4** | **Ảnh, minh họa** |
| IU13.3.4.1 | Biết cách thêm vào, gỡ bỏ một ảnh trên trang web. |
| IU13.3.4.2 | Biết cách đặt, thay đổi thuộc tính cho ảnh như kích thước, biên, căn lề. |
| **IU13.3.5** | **Biểu mẫu** |
| IU13.3.5.1 | Biết cách nhập biểu mẫu (form) lên trang web. |
| IU13.3.5.2 | Biết cách thêm, loại bỏ các trường của biểu mẫu: văn bản (text), hộpthả xuống (drop-down), hộp đánh dấu (check box), nút radio (radio button). Biết cách đặt, thay đổi đặc tính các trường trên. |
| IU13.3.5.3 | Biết cách gửi một kết xuất biểu mẫu qua thư điện tử. |
| **IU13.4** | **CSS (Cascading Style Sheets)** |
| **IU13.4.1** | **Khái niệm CSS** |
| IU13.4.1.1 | Hiểu khái niệm CSS, công dụng và lợi ích của CSS. Biết cách sử dụng các kiểu định dạng (style): trong dòng (inline), bên trong (internal), bên ngoài (external). |
| IU13.4.1.2 | Hiểu cấu trúc của một quy tắc CSS và biết cách áp dụng để chọn và khai báo đặc tính, giá trị. Biết cách tạo, thay đổi quy tắc CSS: màu, nền, phông chữ. |
| IU13.4.1.3 | Biết cách tạo, ghi một tệp CSS mới. |
| IU13.4.1.4 | Biết cách nhúng một CSS ngoài vào trang web. |
| **IU13.5** | **Tải lên máy chủ và phát hành web** |
| **IU13.5.1** | **Kiểm tra** |
| IU13.5.1.1 | Biết cách xác định và xử lý các liên kết bị đứt trong một website. |
| IU13.5.1.2 | Biết cách áp dụng kiểm tra chính tả tự động; biết cách để đảm bảo sự tương thích của nội dung và trình duyệt; biết 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). |
| **IU13.5.2** | **Phát hành** |
| IU13.5.2.1 | Hiểu tiến trình tải nội dung lên máy chủ web, tải một website xuống từ một máy chủ web. |
| IU13.5.2.2 | Biết cách tải lên, tải xuống một website. |

1. **Điểm h, khoản 2, điều 2, số 03/2014/TT-BTTTT: Mô đun kỹ năng 14 (Mã IU14): an toàn, bảo mật thông tin (Bảng 08, Phụ lục số 02):**

| **Mã tham chiếu** | **Nội dung/Yêu cầu cần đạt** |
| --- | --- |
| **IU14.1** | **Kiến thức cơ bản về an toàn thông tin** |
| **IU14.1.1** | **Các nguy cơ mất an toàn thông tin** |
| IU14.1.1.1 | 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. |
| IU14.1.1.2 | 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. |
| IU14.1.1.3 | 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). |
| IU14.1.1.4 | Biết các điểm yếu của máy tính cá nhân (lây nhiễm virus và các phần mềm độc hại - malware). |
| IU14.1.1.5 | 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. |
| **IU14.1.2** | **Các lĩnh vực an toàn thông tin** |
| IU14.1.2.1 | Hiểu 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. |
| IU 14.1.2.2 | Biết các đặc trưng cơ bản của an toàn thông tin: tính mật, tính toàn vẹn, tính sẵn sàng, tính xác thực. |
| IU 14.1.2.3 | Biết các quy định phổ biến về bảo vệ, gìn giữ và kiểm soát dữ liệu, sự riêng tư tại Việt Nam. |
| IU14.1.2.4 | 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. |
| IU14.1.2.5 | 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. |
| **IU14.2** | **Các biện pháp đảm bảo an toàn, bảo mật thông tin, dữ liệu** |
| **IU14.2.1** | **Phòng chống virus** |
| IU14.2.1.1 | 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. |
| IU14.2.1.2 | 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. |
| **IU14.2.2** | **Phòng chống lấy cắp thông tin cá nhân** |
| IU14.2.2.1 | 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. |
| IU14.2.2.2 | 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. |
| IU14.2.2.3 | 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. |
| IU14.2.2.4 | 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). |
| IU14.2.2.5 | 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. |
| **IU14.2.3** | **Đảm bảo an toàn thông tin đối với tài liệu (tệp)** |
| IU14.2.3.1 | Biết tầm quan trọng và hiệu quả của việc thiết lập chế độ an toàn chung (macro security settings). |
| IU14.2.3.2 | Biết tầm quan trọng và cách đặt mật khẩu đối với tệp, tệp tin nén. |
| IU14.2.3.3 | 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. |
| **IU14.3** | **An toàn mạng** |
| **IU14.3.1** | **Các loại tấn công mạng** |
| IU14.3.1.1 | 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. |
| IU14.3.1.2 | 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. |
| IU14.3.1.3 | 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). |
| IU14.3.1.4 | 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. |
| **IU14.3.2** | **Bảo mật mạng không dây** |
| IU14.3.2.1 | 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. |
| IU14.3.2.2 | 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. |
| IU14.3.2.3 | 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). |
| **IU14.3.3** | **Kiểm soát truy nhập (Access Control)** |
| IU14.3.3.1 | 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. |
| IU14.3.3.2 | Hiểu được mục đích của một tài khoản mạng và biết cách sử dụng nó để truy cập mạng. |
| IU14.3.3.3 | 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). |
| IU14.3.3.4 | 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. |
| **IU14.4** | **Sử dụng web an toàn** |
| **IU14.4.1** | **Duyệt web** |
| IU14.4.1.1 | Hiểu sự cần thiết khi thựchiện các giao dịch trực tuyến(mua hàng, giao dịch tài chính) trên các trang webantoàn. Biết các dấu hiệu của một trang web an toàn như https, biểu tượng khóa. |
| IU14.4.1.2 | Biết khái niệm xác thực số. Hiểu lợi ích của mật khẩu dùng một lần. |
| IU14.4.1.3 | Biết cách sử dụng chế độ tự động hoàn chỉnh, tự động lưu khi soạn thảo một biểu mẫu khai trên mạng. |
| IU14.4.1.4 | Hiểu thuật ngữ cookie và biết cách chọn các cài đặt thích hợp để cho phép hoặc ngăn chặn cookie. |
| IU14.4.1.5 | 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). |
| IU14.4.1.6 | 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. |
| **IU14.4.2** | **Mạng xã hội** |
| IU14.4.2.1 | 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. |
| IU14.4.2.2 | Hiểu sự cần thiết phải áp dụng các đặc tính riêng tư cho tài khoản mạng xã hội. |
| **IU14.4.3** | **Thư điện tử** |
| IU14.4.3.1 | Hiểu mục đích của việc mã hóa, giải mã đối với thư điện tử (e-mail). |
| IU14.4.3.2 | Hiểu thuật ngữ chữ ký số. Biết cách tạo và điền một chữ ký số vào thư điện tử. |
| IU14.4.3.3 | Nhận biết nguy cơ từ các thư điện tử không không rõ nguồn gốc. |
| IU14.4.3.4 | 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. |
| IU14.4.3.5 | 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. |
| **IU14.4.4** | **Tin nhắn tức thời** |
| IU14.4.4.1 | 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). |
| IU14.4.4.2 | 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. |
| **IU14.5** | **Quản lý dữ liệu an toàn** |
| **IU14.5.1** | **Bảo vệ vật lý và sao lưu dữ liệu** |
| IU14.5.1.1 | Biết 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. |
| IU14.5.1.2 | 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. |
| IU14.5.1.3 | Biết cách sao lưu dữ liệu. |
| IU14.5.1.4 | Biết cách khôi phục dữ liệu sao lưu và xác nhận dữ liệu. |
| **IU14.5.2** | **Phá hủy dữ liệu an toàn** |
| IU14.5.2.1 | Hiểu được lý do xóa dữ liệu vĩnh viễn từ ổ đĩa hoặc các thiết bị lưu trữ khác. |
| IU14.5.2.2 | Phân biệt giữa việc xóa dữ liệu và hủy dữ liệu vĩnh viễn. |
| IU14.5.2.3 | Biết ưu nhược điểm của các phương pháp hủy dữ liệu vĩnh viễn phổ biến như phá ổ đĩa, dùng công cụ phá hủy. |

1. **THÔNG TIN CÁ NHÂN 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.

*Trường hợp người sử dụng internet dưới 14 tuổi và chưa có hộ chiếu, người giám hộ hợp pháp quyết định việc đăng ký thông tin cá nhân của mình để thể hiện sự cho phép và chịu trách nhiệm trước pháp luật về việc đăng ký đó.*

1. **ĐIỀU 5 NGHỊ ĐỊNH 72/2013/NĐ-CP**

1. Lợi dụng việc cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng nhằm mục đích:

a) 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;

b) 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;

c) 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;

d) Đưa thông tin xuyên tạc, vu khống, xúc phạm uy tín của tổ chức, danh dự và nhân phẩm của cá nhân;

đ) 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;

e) Giả mạo tổ chức, cá nhân và phát tán thông tin giả mạo, thông tin sai sự thật xâm hại đến quyền và lợi ích hợp pháp của tổ chức, cá nhân.

2. Cản trở trái pháp luật việc cung cấp và truy cập thông tin hợp pháp, việc cung cấp và sử dụng các dịch vụ hợp pháp trên Internet của tổ chức, cá nhân.

3. Cản trở trái pháp luật hoạt động của hệ thống máy chủ tên miền quốc gia Việt Nam ".vn", hoạt động hợp pháp của hệ thống thiết bị cung cấp dịch vụ Internet và thông tin trên mạng.

4. Sử dụng trái phép mật khẩu, khóa mật mã của tổ chức, cá nhân; thông tin riêng, thông tin cá nhân và tài nguyên Internet.

5. Tạo đường dẫn trái phép đối với tên miền hợp pháp của tổ chức, cá nhân; tạo, cài đặt, phát tán phần mềm độc hại, vi-rút máy tính; xâm nhập trái phép, chiếm quyền điều khiển hệ thống thông tin, tạo lập công cụ tấn công trên Internet.

1. **THỎA THUẬN CUNG CẤP VÀ SỬ DỤNG DỊCH VỤ:**

**Các nội dung chính**

* Các nội dung cấm trao đổi, chia sẻ trên mạng xã hội;
* Quyền, trách nhiệm của người sử dụng dịch vụ mạng xã hội;
* Quyền, trách nhiệm của tổ chức, doanh nghiệp thiết lập mạng xã hội;
* Cơ chế xử lý đối với thành viên vi phạm thỏa thuận cung cấp và sử dụng dịch vụ mạng xã hội;
* Cảnh báo cho người sử dụng các rủi ro khi lưu trữ, trao đổi và chia sẻ thông tin trên mạng;
* Cơ chế giải quyết khiếu nại, tranh chấp giữa các thành viên mạng xã hội với tổ chức, doanh nghiệp thiết lập mạng xã hội hoặc với tổ chức, cá nhân khác;
* Công khai việc có hay không thu thập, xử lý các dữ liệu cá nhân của người sử dụng dịch vụ trong thỏa thuận cung cấp và sử dụng dịch vụ mạng xã hội;
* Chính sách bảo vệ thông tin cá nhân, thông tin riêng của người sử dụng dịch vụ mạng xã hội.

**NỘI DUNG CHI TIẾT PHƯƠNG ÁN KỸ THUẬT**

1. **Thành lập Bộ phận kỹ thuật**
2. **Thành phần**

* Bộ phận kỹ thuật gồm ... người, được ký hợp đồng vô thời hạn sau khi thử việc ... tháng.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| STT | Họ và tên | Chức danh | Kinh nghiệm | Bằng cấp/chứng chỉ |
| 1 | Nguyễn Văn A | Trưởng Bộ phận |  |  |
| 2 | Nguyễn Văn B | Phó Bộ phận |  |  |
| 3 | Nguyễn Văn C | Cố vấn |  |  |
| 4 | Nguyễn Văn D | Chuyên viên |  |  |
| 5 | Nguyễn Văn E | Chuyên viên |  |  |

* Các văn bằng, chứng chỉ của các thành viên Bộ phận kỹ thuật đính kèm

1. **Nhiệm vụ cụ thể của Bộ phận kỹ thuật như sau:**

+ Thiết kế giao diện

+ Thiết kế module chức năng

+ Mua/tìm đối tác ký hợp đồng thuê các thiết bị kỹ thuật cần thiết để vận hành website

+ Thiết lập cơ chế vận hành của website, quy trình theo dõi việc vận hành, xử lý sự cố đảm bảo website vận hành một cách an toàn, liên tục

+ Thiết lập quy trình nhận thông tin và phản hồi cho user, cơ quan chức năng khi có có yêu cầu.

+ Trưởng Bộ phận có trách nhiệm giám sát đôn đốc cấp dưới thực hiện tốt nhiệm vụ của Bộ phận

+ Cố vấn là thành viên độc lập, có nhiệm vụ tư vấn cơ chế, quy trình, giải pháp giúp website hoạt động an toàn, liên tục

+ Cấp dưới thực hiện nhiệm vụ cho Trưởng Bộ phận giao, đồng thời có trách nhiệm tham mưu, tư vấn cho trưởng Bộ phận những giải pháp thiết thực, hiệu quả giúp website vận hành an toàn, liên tục.

1. **Các thiết bị kỹ thuật**

* Do Bộ phận kỹ thuật quyết định việc mua/thuê dựa trên đánh giá kỹ lưỡng về hiệu quả sử dụng cũng như hiệu quả về mặt tài chính.
* Các thiết bị kỹ thuật gồm

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| STT | Tên thiết bị | Chức năng | Cấu hình | Số lượng |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| ... |  |  |  |  |

* Chi tiết theo Hợp đồng Mua/Thuê đính kèm.

1. **Thiết kế, vận hành website**
2. **Cơ chế đăng nhập**

* Kê khai thông tin: tên, username, email
* Đồng ý sử dụng dịch vụ, cho phép hiển thị sử dụng thông tin cá nhân,
* Gửi mail xác thực
* Thông báo xác nhận mở tài khoản tới user
* Hướng dẫn điền đầy đủ các thông tin còn thiếu trong phần Setting/Profile

...

...

...

1. **Cơ chế đăng bài viết**

* Ngay khi user nhập các ký tự tại module viết bài, hệ thống sẽ tự động kiểm duyệt các nội dung vi phạm và sẽ có báo cáo ngay khi user post bài
* Các user có thể báo cáo bài viết vi phạm của user khác và hệ thống sẽ tự động tổng hợp và bộ phận chịu trách nhiệm nội sẽ xử lý các bài viết thực sự vi phạm nội dung
* Đối với những nội dung mà hệ thống tự động kiểm duyệt không nhận thấy sự vi phạm thì bộ phận kiểm duyệt nội dung sẽ thực hiện rà soát và kiểm duyệt nội dung 24/24.

...

...

...

1. **Cơ chế xử lý đối với những bài viết, user vi phạm**

* Tự động xóa
* Ban nick
* Xóa nick

...

...

...

1. **Cơ chế ngăn chặn hành vi xâm phạm bất hợp pháp**

* Các loại hành vi xâm phạm
* Những hình thức xâm phạm
* Những thiệt hại có thể xảy ra nếu website bị xâm phạm
* Cơ chế, quy trình ngăn chặn
* Mức độ hiệu quả của cơ chế, quy trình ngăn chặn

...

...

...