**E-Guard**

**Client Project Requirement Capture**

**Due: 10/15/2013**

**By:**

**Jaime Cedillo**

**Cas Dusute**

**Jeff Klanderman**

**Lisa Snyder**

**Table of Contents**

Revision History . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3

Project Requirements Capture Deliverables/Schedule . . . . . . . . . . . . . . 4

Current Situation . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 5

Statement of Work . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 5

Scenarios. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .6

Functional Requirements. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .8

Nonfunctional Requirements. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .8

Use Cases. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .9

Project Schedule . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .12

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Change/Comments** |
| **0.0.1** | **10/13/2013** | CD, JC, JK, LS | **Initial revision** |
|  |  |  |  |

**Project Requirements Capture Deliverables/Schedule**

|  |  |
| --- | --- |
| **Description** | **Complete Date** |
| Requirement Capture Document | 10/11/2013 |
| Powerpoint Presentation | 10/12/2013 |
| Team Review (during team meeting) | 10/13/2013 |
| Assign Presenter (during team meeting) | 10/13/2013 |
| Upload Document/Presentation to Repository | 10/14/2013 7:00pm |
| Project Requirement Capture Review/Presentation (during class) | 10/15/2013 |

**Deliverables**

* Problem Description
  + The current situation
  + Statement of Work
  + Functional Requirement
  + Nonfunctional Requirement (usability, reliability, performance,supportability)
* Scenarios
* Use Case
* Project Schedule
* Powerpoint Presentation

**Notes**

Problem description is a simple statement of what the product should do and not how to do it.

Scenarios to Use Cases ratio is 2 to 1.

30-40% of functional requirements should have scenarios and use cases

**Current Situation**

It is far too easy for children to gain access to inappropriate subject matter and dangerous sites on the web and it is no easy task for parents to protect their children from these risks. Parents’ need a way to enforce parental control policies. Parents need to be kept informed of childrens’ inappropriate internet usage and behavior on the computer. Parents need to have the ability to block children from inappropriate sites, be informed of possible inappropriate language and limit the amount of time children are spending on the internet.

**Statement of Work**

The project entails the development of an application to allow parents to monitor children’s web activity and be informed of children’s inappropriate language. It will also allow the parents to block undesirable websites and limit internet usage time.

This project will require a team of 4 developers. The time required to complete the project is approximately 11 weeks. The team will deliver a completed and tested stand-alone application by 12/15/2013.

In order to reach decisions to support program timing and to identify issues and tasks, the development team will meet weekly to review status and identify/resolve issues. There is geographic distance between the the team members. Due to this distance, the team will use Skype to conduct the weekly meetings.

Each team member will require a development computer with internet access and will require Visual Studio 2010 to be installed. The team will provide project requirements by 10/15/2013, architecture and design by 11/6/2013 and the completed application by 12/11/2013. The team will be prepared to demo the application for the customer on 12/15/2013.

**Scenarios**

Bob and Alice will be parents, Charlie can be the kid.

Scenario Example: Configuration

Bob and Alice want to monitor the web activity of their child, Charlie. To do so, they install E-Guard Client.

After installing the client, they configure E-Guard by creating an Admin username and password. This will allow them access to the Admin Activities page.

From there, they can blacklist websites, words, add time limits and choose safe categories for Charlie’s user account.

Scenario Example: Blacklist website

Bob and Alice allow Charlie to use the computer for an hour a day. They noticed that Charlie was visiting an unhealthy website. They decide to blacklist the site.

From E-Guard, Bob enters the URL of the unhealthy website into the Blacklist and confirms the add.

A screenshot will be provided whenever Charlie tries to access the blacklisted site.

Scenario Example: Unblacklist website

Bob and Alice decide that Charlie is old enough to go to a Blacklisted site.

From E-Guard, Bob and Alice click on the Blacklisted Sites, and choose the URL of the site they want to unblock.

Charlie will be able to visit the site now.

Scenario Example: Email

Charlie’s vocabulary has been evolving, much to Bob and Alice’s dismay. To prevent Charlie from using foul language, they decide to monitor his activity.

From E-Guard, Alice enters multiple words that Charlie has been using lately into the Blacklisted words area, and confirms the add. In addition, she also requests a log to be sent whenever Charlie uses the words in an email.

Along with a log, Alice and Bob will also receive a screenshot whenever Charlie uses one of the Blacklisted words in an email.

Scenario Example: Chat

From E-Guard, Alice enters multiple words that Charlie has been using lately into the Blacklisted words area, and confirms the add. In addition, she also requests a log to be sent whenever Charlie uses the words in chat.

Alice and Bob will also receive a screenshot whenever Charlie uses one of the Blacklisted words in chat.

Scenario Example: Search

Charlie enters search criteria that includes inappropriate language. Before the search is conducted, a screenshot is captured and the inappropriate words are stripped from the search. The screenshot is sent to the web server.

Scenario Example: Whitelist

Bob and Alice want to be able to specify kid-friendly websites that Charlie can visit. Bob and Alice specify the approved websites in a whitelist. When Charlie visits one of these websites included on the white list, he will be able to visit the site.

Scenario Example: Categories

Bob and Alice want to block website categories that are unfit for Charlie to visit. They are given a list of categories they can choose to block. When Charlie visits one of the websites in the blocked category he is notified that the website is blocked and will be unable to access the site.

Scenario Example: Internet Time Control

Bob and Alice have limited Charlie’s internet usage to 1 hour a day. However, they do not feel comfortable leaving it to Charlie to abide by the rule on his own, so Bob accesses the configuration setting of E-Guard and updates the internet time control equal to 1 hour limiting Charlie to 1 hour. Once Charlie reaches the 1 hour time limit, he will not be permitted to surf the internet.

Scenario Example: Uninstallation

Bob and Alice installed E-Guard and do not want anyone other than them to uninstall the application. When uninstallation is attempted, Bob and Alice want to make sure they are the only users than can complete the uninstall. If Charlie attempts the uninstall, he should not be permitted.

To prevent Charlie from uninstalling, Bob and Alice set up a username and password for the E-Guard program. If Charlie tries to uninstall, he will have to enter these credentials.

**Functional Requirements**

1. The monitoring function shall allow parents to check web activity, keystroke, chat, email, IM and launched application and send the log to the web team server in the real time.

2. The client shall keep a local DB of unhealthy websites and synchronize the DB with the server team in a daily basis. (note: it is web team’s responsibility to create and maintain the central DB)

3. The client shall block unhealthy websites

4. The client shall remove unhealthy words from search engine (note: it is web team’s responsibility to create and maintain common unhealthy keywords)

5. Once a suspicious activity is identified, the client shall take snapshot of the screen and notify the web team’s server. The suspicious activities include trying to browse unhealthy websites, nasty words appear in email/chat/IM or typing blocked keywords in search engine.

6. The client shall allow parents to configure the setting. The setting includes, blacklist, whitelist, blocked keyword, internet time control, categories to be blocked (it is web team’s responsibility to create and maintain the website categories), etc

7. Only authorized users have access to the configuration and uninstall.

**Nonfunctional Requirements**

* Application should run on Windows, Linux, and MAC environments
* Synchronize with web team server daily
* Application should be available 24 hours a day 7 days a week
* User input should result in a response within seconds
* Graphical user interface should be user friendly and intuitive
* User should be unaware that application is running
* Future updates should be easy to install

**Use Cases**

**Use Case Name:** BlockedCategores

Participant Actors:   
Parents (Bob and Alice in the Scenarios)

WebDB (Subsystem)

Client (E-Guard Client)

Flow of Events:

1. Parents want to block a group of websites that contain unhealthy information to prevent family members from accessing them. Parents activate the BlockedCategories function of e-Guard client.
2. WebDB subsystem receives a request to provide the current website categories.
3. Parents are presented with a list of categories from which they are able to select the category to be blocked.
4. Parents select the “Violence” category from the list.
5. Parents are asked to confirm the selected category.
6. Parents confirm the information
7. Parents receive a notification saying that the category has been added to the blocked categories group.

**Use Case Name:** Blacklist

Participant Actors:

Parents (Bob and Alice in the Scenarios)

Child (Charlie in the Scenarios)

WebDB (Subsystem)

Client (E-Guard Client)

Flow of Events:

1. Parents know about a web site with unhealthy content that is frequently visited by Child. Parents want to prevent the access to this web site and activates the Blacklist function of Client.
2. Parents select the Client Blacklist form and enters the URL of the web site in one of the fields.
3. Parents are asked to confirm the URL to be added to the blacklist.
4. Parents confirm that the URL is correct.
5. Parents receive a notification saying that the URL has been added to the blacklist.
6. Parents are presented with an updated blacklist.

**Use Case Name:** Whitelist

Participant Actors:

Parents (Bob and Alice in the Scenarios)

Child (Charlie in the Scenarios)

Client (E-Guard Client)

Flow of Events:

1. Parents want to allow access to a web site and track the time that Child spends on it. To do that, Parents activate the Whitelist function of Client.
2. Parents select the Client Whitelist form and enters the URL of the web page in one of the fields.
3. Parents are asked to confirm the URL to be added to the whitelist.
4. Parents realize that there is an error in the URL and cancels the addition.
5. Parents receive a notification saying that the URL has not been added to the whitelist.
6. Parents correct the mistake and adds the URL to the white list again.
7. Parents are asked to confirm the URL to be added to the white list.
8. Parents confirm that the URL is correct now.
9. Parents receive a notification saying that the URL has been added to the whitelist.

**Use Case Name:** InternetTimeControl

Participant Actors:

Parents (Bob and Alice in the Scenarios)

Child (Charlie in the Scenarios)

Client (E-Guard Client)

Flow of Events:

1. Parents want to restrict the time that Child spends on Internet on a daily basis and activates the InternetTimeControl function of Client.
2. Parents select the user account of Child from the user list.
3. Parents are presented with a form to configure Internet Time restrictions.
4. Parents enter the “Start time” and “End time” in the appropriate fields of the form.
5. Parents are asked to confirm the information.
6. Parents confirm that the information is correct.
7. Parents receive a notification saying that the time restrictions have been applied to the user account.

**Use Case Name:** UninstallClient

Participant Actors:

Parents (Bob and Alice in the Scenarios)

Child (Charlie in the Scenarios)

Client (E-Guard Client)

Flow of Events:

1. Parents want to uninstall Client application from one of the computers. Parents activate the AdminAuthentication function of Client.
2. Parents are presented with a form to enter his user ID and password.
3. Parents enter the User ID and Password correctly.
4. Parents are presented with a list of administration activities including the option to uninstall Client.
5. Parents select the option “UninstallClient”.
6. Parents are asked to confirm the uninstallation.
7. Parents confirm the selected option.
8. Parents receive a notification saying that Client is being uninstalled and progress of the uninstallation.
9. Parents confirm the end of the uninstall process once it has been completed.

**Use Case Name:** Search

Participant Actors:

Child (Charlie in the Scenarios)

Client (E-Guard Client)

WebDB (Subsystem)

Flow of Events

1. Child initiates a search containing an inappropriate word in the search criteria
2. The inappropriate words are matched to a list of blacklisted words
3. As Child types the search, the screenshot is taken
4. The search string typed by Child initially is modified to exclude the bad words
5. The screenshot is sent to the WebDB

**Project Schedule**

