Software Requirements Specification

**Abuse Reporting System**

Sihao Chen, Cheng Deng, Kexin Liu, Guanxiong Liu, Chao Ren, Hao Zhou

Worcester Polytechnic Institute

CS 509 Design of Software Systems

Professor Erik Hemdal

02/20/2014

Table of Contents

[Software Requirements Specification 1](#_Toc31276)

[Abuse Reporting System 1](#_Toc30237)

[Sihao Chen, Cheng Deng, Kexin Liu, Guanxiong Liu, Chao Ren, Hao Zhou 1](#_Toc1011)

[Worcester Polytechnic Institute 1](#_Toc27427)

[CS 509 Design of Software Systems 1](#_Toc617)

[Professor Erik Hemdal 1](#_Toc6466)

[02/20/2014 1](#_Toc13608)

[Table of Contents 2](#_Toc7385)

[1. Introduction 3](#_Toc23952)

[1.1 Purpose 3](#_Toc30264)

[1.2 Scope 3](#_Toc5441)

[1.3 Definitions, acronyms, and abbreviations 4](#_Toc20691)

[1.4 References 5](#_Toc6408)

[1.5 Overview 5](#_Toc16601)

[2. Overall Description 5](#_Toc13446)

[2.1 Product perspective 5](#_Toc4817)

[2.2 Product functions 6](#_Toc7142)

[2.3 User characteristics 7](#_Toc25844)

[2.4 Constraints 8](#_Toc11347)

[2.5 Assumptions and dependencies 8](#_Toc16460)

[3. Specific Requirements 8](#_Toc4369)

[3.1 External interface requirements 8](#_Toc22504)

[3.1.1 User interfaces 8](#_Toc31329)

[3.1.2 Hardware interfaces 11](#_Toc1705)

[3.1.3 Software interfaces 11](#_Toc15523)

[3.2 Functional requirements 11](#_Toc10353)

[3.2.1 User Class 1 – Direct Support Staff 11](#_Toc8519)

[3.2.2 User Class 2 – Supervisor 12](#_Toc4531)

[3.2.3 User Class 3 – Chairman of Human Rights Committee 14](#_Toc16530)

[3.2.4 User Class 4 – Administrator 16](#_Toc16577)

[3.3 Performance requirements 17](#_Toc12865)

[3.4 Design constraints 20](#_Toc32328)

[3.5 Software system attributes 21](#_Toc5263)

[3.6 Other requirements 24](#_Toc3795)

# Introduction

This introduction section states the project scope and gives an overview of everything included in this Software Requirements Specification (SRS) document. This section also describe the purpose of this document and provide a list of abbreviations and definitions.

## Purpose

The purpose of this document is to give a detailed description of the requirements for the “Abusing Reporting System” (ARS). This SRS document is intended to provide the environmental and software functional requirements for ARS. It will also explain system constraints, interface and interactions with other external applications. It will serve as a reference for the design phase, as well as an agreement with the customer as to the exact specifications of the system.

## Scope

This “Abusing Reporting System” is a cross-platform application for computers, tablets and smartphones. It allows direct support staffs from health care organizations (agency) that provides programming to individuals with severe developmental and mental health issues enter patient information about abuse incidents as soon as they happen.

The system shall be accessed only by authorized users. Only the agency’s supervisors can review, correct, and add information to the abuse report that input by the direct support staffs using this application. The application provides supervisors a list and a calendar of active reports, their status, action dates and their deadlines. All inactive or complete reports should be archived, and all users’ activities should be logged and tracked by an audit trail for monitoring and troubleshooting for a limited time based on established retention criteria.

The application should be able to redact information that should not be displayed or preserved, such as, the names of alleged victims and alleged abusers. It also help users verify that all necessary information is provided.

After an investigator is assigned to the abuse case, the application needs the capability of tracking investigation progress. Each investigation is assigned a unique public log number. The human resources officers should be able to save all scanned copies of disposition letters, responses, and decision letters for each investigation. The human resources officers and the chairman of Human Rights Committee have the ability to review the abuse report and change the status of abuse cases.

## Definitions, acronyms, and abbreviations

This section defines the terms needed to properly interpret this document:

**Administrator:** System administrator who is given specific permission for managing and controlling the system. The system access privileges of direct support staffs, supervisors, and members of human rights committee are granted by system administrator.

**Agency:** Agency is the health care organization that provides both day and residential programming to individuals with severe developmental and mental health issues.

**ARS (Abuse Reporting System):** Abuse reporting system is a cross-platform application that allows direct support staffs enter patient information about abuse incidents as soon as they happen.

**Customer:** Customer is a health care organization that provides both day and residential programming to individuals with severe developmental and mental health issues.

**DEP:** Dependency

**DESC:** Description

**Direct Support Staff:** Direct Support Staff are the people who are trained to care for the individuals with severe developmental and mental health issues.

**RAT:** Rational

**SRS (Software Requirements Specification):** This document.

**Supervisor:** Supervisors are the managers who can review, correct, and add information to the abuse report.

## References

1. IEEE Software Engineering Standards Committee (1998), “IEEE Std 830-1998, IEEE Recommended Practice for Software Requirements Specifications”.

2. Geagea, S., Zhang, S., Sahlin, N., Hasibi, F., Hameed, F., Rafiyan, E. and Ekberg, M. (2010).

3. Software Requirements Specification - Amazing Lunch Indicator. [E-book]

4. http://www.cse.chalmers.se/~feldt/courses/reqeng/examples/srs\_example\_2010\_group2.pdf

5. Bruegge, B. & Dutoit, A. (2010). Object-oriented software engineering: using UML, patterns,

And Java. Boston: Prentice Hall.

## Overview

This document consists of three sections:

The first section (Introduction) states the project scope and gives an overview of everything included in this SRS document.

The second section gives an overview of the system and details of the system functionality. It also provide the system constraints and assumptions about the product.

The third section describes the specific functional requirements and the system interfaces. The functional requirements are organized by user class in order to specify the different sets of functions to different classes of users precisely.

# Overall Description

This section gives an overview of the system and details of the system functionality. It also provide the system constraints and assumptions about the product.



## Product perspective

The system will mainly consist of two parts: applications on different kind of devices and central computer. The application will be used to input the original report, modify the existing report, tracking the progress of abuse incidents and interact with the central computer. The central computer will be responsible for storing all reports and related documents. All of interaction between the application and central computer will be based on Internet access.

Specifically, the application should be able to run on different devices, such as laptops, tablets and cellphone, so that the abuse incident can be reported in time. Moreover, the application will have some functions to interact with central computer, including setting up account, report input, report review and revise and tracking status of reports. The application will enable users to register for an account, a user name and a password. Meanwhile, questions and corresponding answers can be set in case that they forget their passwords. After the registration, the system will assign different users different permission to the system.

After the report is typed in, the application will verify information in the report. The report can be submitted if all required information is provided in the report. The application will be able to remove all the confidential information in the report, such as the victim’s name and the abuser’s name. Then the report will be sent to the central computer for future use. By typing in the Public Log Number on application, the investigation can be tracked.

The central computer will provide the supervisors permission to view the list of active reports and their status. If an appeal is requested for an incident, it will also show on this list. In addition, the system can provide hard copy of initial reports for mail, fax or other use when connected to a printer. With the investigation going on, the system will be able to scan and save all related documents in a file for each abuse incident. Each active abuse incident investigation will be marked on a calendar, displaying the action dates and deadline for requesting appeals. The central computer will also keep the record of user access to the system. According to retention rules, the central computer can remove documents.

## Product functions

This application allows direct support staffs from agency enter patient information about abuse incidents as soon as they happen from multi-platform including computers, tablets and smartphones.

With the abuse incidents reports, authorized users can review, correct, and add information to the abuse reports using this application. The system provides authorized users a list and a calendar of active reports, their status, action dates and their deadlines. The system and its audit trail will archive all inactive or complete reports, and log all users’ activities for a limited time based on established retention criteria.

The application will be able to redact information that should not be displayed or preserved, such as, the names of alleged victims and alleged abusers. It will also help users verify that all necessary information is provided.

After an investigator is assigned to the abuse case, the application has the capability of tracking investigation progress. Each investigation will be assigned a unique public log number. The authorized users will be able to save all scanned copies of disposition letters, responses, and decision letters into this system for each investigation. The authorized users also have the ability to change the status of abuse cases.

## User characteristics

There are three types of users that interact with the system: staff, supervisor, member of the agency’s Human Rights Committee. Each of these three types of users interacts with the system differently so each of them has their own requirement.

The direct support staff users input pertinent information about incident into system as soon as it happens. Then the system produces an abuse report and send to all necessary staff member of the agency.

The supervisor user can use the system to review, correct, and add information to a report before it is sent to the DPPC. Then supervisor should input Disposition letter, Decision letter and other documents. Supervisor user also use the system to view the virtual investigation file and calendar display, to track the status of abuse reports (list of active reports and their status)

Human Rights Committee user uses the system to review the documents, and input the decision of the appeal.

## Constraints

The Abusing Report System is constrained by the Massachusetts regulatory policies concerning persons with developmental disabilities, or policies concerning privacy and human rights. The system should protect the right of the clients as well as protect the staff from being subjected to unwarranted disciplinary actions.

The internet connection is also a constraint for the application. Since the application fetches data from the database over the Internet, it is crucial that there is an Internet connection for the application to function.

## Assumptions and dependencies

One assumption about the system is that it should be well applied to all devices: it will be used on smart devices such as computer, laptop, cell phone or tablet PC. And the interface and function of the system should be specifically adjusted to each device.

One dependence is that the system needs the administrator input the documents and information in time, so that the user can make use of the system.

# Specific Requirements



## External interface requirements

This section provides a detailed description of all inputs into and outputs from the system. It also provides basic prototypes of the user interface, and gives a description of the hardware, software and communication interfaces.

### User interfaces

As the system will not allow users signing up by themselves, there will be some top administrators, who can create new users, initialized with this system.

In Figure 1, the administrator can create new user with role information, then a random password, which can be changed later after user’s login, will be sent to the new user’s email.

In Figure 2, when user logins in, the system can identify his/her role, and then provide the user interfaces based on the role (Different roles have different permissions). Sometimes, user may forget his password, in this case, the system provides “password reset” feature as Figure 3, which can send a password reset link to the user’s email.

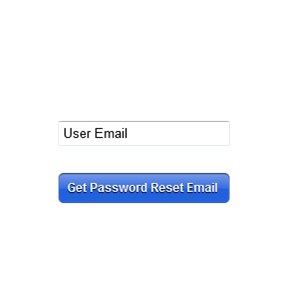
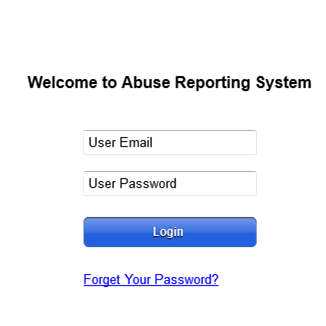
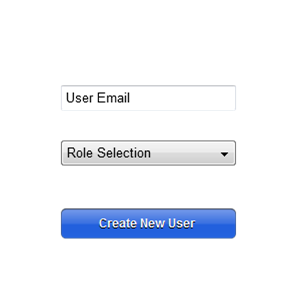


Figure 1: User Create Figure 2: User Login Figure 3: Password Reset

As Figure 4, the direct staff can submit an abuse report after login (The input fields may be more than provided in figure 4 at final project).



Figure 4: Abuse Report

In Figure 5, after login, the supervisor will see a list of abuse reports. He/she can click the title field to review the detailed information. Also, he/she can correct, and add information to a report, then mail it to DCCP, as shown in Figure 6.



Figure 5: Abuse Report List Review

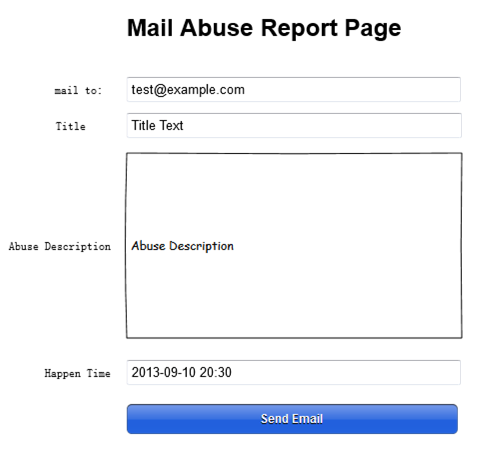


Figure 6: Abuse Report Email to DPPC

Actually, above are just parts of user interfaces, and the system will be more complex in details.

### Hardware interfaces

Since we will make a web-based system, there is no direct hardware interface.

### Software interfaces

We will setup the Web server and database server in the same computer, which will simplify the communication between different servers. The communication between the database and the web consists of operation concerning both reading and writing the data. As the system will provide email sending service, an email server is needed. Even the email sending server is apart, it provides email sending API, which can be called in web server.

## Functional requirements

### User Class 1 – Direct Support Staff

* + - 1. Functional requirements 1.1

ID: FR1

TITLE: Register to the system

DESC: A direct staff should be able to register his or her account in the system with the default user name and password from the system administrator

RAT: In order for a user to set his or her own user name and password

DEP: None

* + - 1. Functional requirements 1.2

ID: FR2

TITLE: Login the system

DESC: A direct staff should be able to login his or her account in the system with the user name and password

RAT: In order for a user to login the system after register

DEP: FR1

* + - 1. Functional requirements 1.3

ID: FR3

TITLE: Produce and save abuse report draft

DESC: A direct staff should be able to create his or her report in the system and save the draft

RAT: In order for the direct staff to type in the needed information to the report

DEP: FR2

* + - 1. Functional requirements 1.4

ID: FR5

TITLE: Submit a report

DESC: A direct staff should be able to submit his or her report draft to the system

RAT: None

DEP: FR3 and FR4

* + - 1. Functional requirements 1.5

ID: FR6

TITLE: Remove a report draft

DESC: A direct staff should be able to remove a report draft from the system

RAT: In order for a direct staff remove the wrong and not submitted report

DEP: FR3

### User Class 2 – Supervisor

* + - 1. Functional requirements 2.1

ID: FR7

TITLE: Register to the system

DESC: A supervisor should be able to register his or her account in the system with the default user name and password

RAT: In order for a user to set his or her own user name and password

DEP: None

* + - 1. Functional requirements 2.2

ID: FR8

TITLE: Login the system

DESC: A supervisor should be able to login his or her account in the system with the user name and password

RAT: In order for a user to login the system after register

DEP: FR7

* + - 1. Functional requirements 2.3

ID: FR9

TITLE: Review the report

DESC: A supervisor should be able to review the report

RAT: In order for the user to review the report which is sent to him or her

DEP: FR8

* + - 1. Functional requirements 2.4

ID: FR10

TITLE: Correct the report

DESC: A supervisor should be able to correct the report

RAT: In order for the user to correct the report which is sent to him or her, and the system will save an original file before correction

DEP: FR8

* + - 1. Functional requirements 2.5

ID: FR11

TITLE: Add information to a report

DESC: A supervisor should be able to add material to the report

RAT: In order for the user to add all kinds of necessary material to the report

DEP: FR8

* + - 1. Functional requirements 2.6

ID: FR13

TITLE: Print out

DESC: A supervisor should be able to print out any necessary material

RAT: In order for the user to print out the material to use

DEP: FR8

* + - 1. Functional requirements 2.7

ID: FR14

TITLE: Upload Disposition Letter

DESC: A supervisor should be able to upload the Disposition Letter to a related report

RAT: None

DEP: FR8

* + - 1. Functional requirements 2.8

ID: FR15

TITLE: Upload Decision Letter

DESC: A supervisor should be able to upload the Decision Letter to a related report

RAT: None

DEP: FR8

* + - 1. Functional requirements 2.9

ID: FR16

TITLE: Upload investigation report

DESC: A supervisor should be able to upload the investigation report to a related report case

RAT: None

DEP: FR8

* + - 1. Functional requirements 2.10

ID: FR17

TITLE: Track investigation report

DESC: A supervisor should be able to track the investigation report by Public Log Number

RAT: None

DEP: FR8

### User Class 3 – Chairman of Human Rights Committee

* + - 1. Functional requirements 3.1

ID: FR18

TITLE: Register to the system

DESC: A chair of Human Rights Committee should be able to register his or her account in the system with the default user name and password from the system administrator

RAT: In order for a user to set his or her own user name and password

DEP: None

* + - 1. Functional requirements 3.2

ID: FR19

TITLE: Login the system

DESC: A chair of Human Rights Committee should be able to login his or her account in the system with the user name and password

RAT: In order for a user to login the system after register

DEP: FR7

* + - 1. Functional requirements 3.2

ID: FR20

TITLE: Review the report

DESC: A chair of Human Rights Committee should be able to review the report and its all related material

RAT: In order for the user to review the report

DEP: FR19

* + - 1. Functional requirements 3.3

ID: FR21

TITLE: Track investigation report

DESC: A chair of Human Rights Committee should be able to track the investigation report by Public Log Number

RAT: None

DEP: FR19

* + - 1. Functional requirements 3.4

ID: FR22

TITLE: Print out

DESC: A chair of Human Rights Committee should be able to print out whole material within a report case

RAT: In order for the user to print out the material to use

DEP: FR19

* + - 1. Functional requirements 3.5

ID: FR23

TITLE: Change the status of abuse report to appeal

DESC: A chair of Human Rights Committee should be able to change the status to appeal

RAT: None

DEP: FR19

* + - 1. Functional requirements 3.6

ID: FR23

TITLE: Upload the result of appeal

DESC: A chair of Human Rights Committee should be able to upload the result of the appeal

RAT: None

DEP: FR19

### User Class 4 – Administrator

* + - 1. Functional requirements 4.1

ID: FR24

TITLE: Login the system

DESC: An administrator should be able to login his or her account in the system with the user name and password

RAT: In order for a user to login the system

DEP: FR7

* + - 1. Functional requirements 4.2

ID: FR25

TITLE: Manage direct staff user

DESC: An administrator should be able to manage direct staff user

RAT: In order for a user to manage the database of direct staff user

DEP: FR24

* + - 1. Functional requirements 4.3

ID: FR26

TITLE: Manage supervisor user

DESC: An administrator should be able to manage supervisor user

RAT: In order for a user to manage the database of supervisor user

DEP: FR24

* + - 1. Functional requirements 4.4

ID: FR27

TITLE: Manage chair of Human Rights Committee user

DESC: An administrator should be able to manage chair of Human Rights Committee user

RAT: In order for a user to manage the database of chair of Human Rights Committee user

DEP: FR24

* + - 1. Functional requirements 4.5

ID: FR27

TITLE: Add user

DESC: An administrator should be able to add the user in any of the user database

RAT: In order for a user to add new user to the user database

DEP: FR24

* + - 1. Functional requirements 4.6

ID: FR27

TITLE: Delete user

DESC: An administrator should be delete to add the user in any of the user database

RAT: In order for a user to delete new user to the user database

DEP: FR24

## Performance requirements

3.3.1 Prominent reporting feature

ID: QR1

Title: Prominent reporting feature

DECS: The reporting form should be prominent, easy to find and easy to fill in for the staff user.

RAT: In order to for a staff user to find the reporting form and fill in easily.

DEP: none

3.3.1 Usage of submit result notification

ID: QR2

Title: Usage of submit result notification

DECS: After staff user submitted the report, the submit notification should be prominent and easy to understand.

RAT: In order to for a staff user to know the report is successful submitted or not easily and clearly.

DEP: none

3.3.2 Report modification feature

ID: QR3

Title: Report modification feature

DECS: The report submitted by staff user should be easy to find and modified by the supervisor.

RAT: In order to for a supervisor to view and modify reports easily.

DEP: none

3.3.3 Report tracking feature

ID: QR4

Title: Report tracking feature

DECS: The active reports should be viewed and status of which be tracked easily by the supervisor.

RAT: In order to for a supervisor to view and track active reports easily.

DEP: none

3.3.4 Administrator feature

ID: QR5

Title: Administrator feature

DECS: The administrator should be able to add or delete user account easily

RAT: In order to for an administrator to manage user account easily.

DEP: none

3.3.5 Response time

ID: QR6

Title: Response Time

GIST: The fastness of the response of the system when submitting a report.

DESC: The response time of a report submitting operation.

METER: Measurements obtained from 100 times report submit during testing.

MUST: No more than 3 seconds 100% of the time.

WISH: No more than 2 seconds 100% of the time.

3.3.6 System dependability

ID: QR7

Title: System Dependability

GIST: The fault tolerance of the system.

SCALE: If the terminal loses the connection to the Internet or due to some reason the terminal can’t connect to the server, the user should be informed.

METER: Measurements obtained from 100 hours of usage of testing.

MUST: 100% of the time.

Terminal: DEFINED: The device which the accessing the system.

## Design constraints

3.4.1 Central computer hard drive space

ID: QR8

TAG: CentralComputerHardDriveSpace

GIST: Central computer hard drive space

SCALE: The system‘s need of hard drive space in the central computer of the agency.

METER: MB

MUST:

PLAN:

WISH:

MB: DEFINED: Megabyte

3.4.2 Central computer memory usage

ID: QR9

TAG: CentralComputerMemoryUsage

GIST: The memory usage of the system on the central computer of the agency.

SCALE:

METER:

MUST:

PLAN:

WISH:

## Software system attributes

3.5.1 Reliability

ID: QR10

TAG: SystemReliability

GIST: The reliability of the system.

SCALE: The reliability that the user submitting reports or view documents via the system.

METER: Measurements obtained from 100 times report submit and documents opening.

MUST: More than 95% of the time.

PLAN: More than 98% of the time.

WISH: 100% of the time.

3.5.2 Availability

ID: QR11

TAG: SystemAvailability

GIST: The availability of the system when it is used.

SCALE: The average system availability (not considering network or web browser failing).

METER: Measurement obtained from 100 hours of usage during testing.

MUST: More than 98% of the time.

PLAN: More than 99% of the time.

WISH: 100% of the time.

3.5.3 Security

ID: QR12

TAG: Communication Security

GIST: Security of the communication between the users and server.

SCALE: The message should be encrypted for log-in communications, so that others can’t get any information about the account, user-name or password from log-in messages.

METER: Attempts to get user-name and password through obtained messages on 100 log-in session during testing.

MUST: 100% of the communication messages in a log-in session should be encrypted.

ID: QR13

TAG: Document Security

GIST: Security of documents and changes that make to the reports transmitting between users and server.

SCALE: Reports and all kind of documents including disposition letter, responds, decision letter should be encrypted in transmission, so that others can’t get any information through these transmission.

METER: Attempts to get the document transmitting in the system by eavesdropping for 100 times during testing.

MUST: 100%of the documents transmitting in the system should be encrypted.

ID: QR15

TAG: Account Security

GIST: Security of accounts.

SCALE: An IP address should not be able to log-in to any account for a certain time period after three times of failed log-in attempts.

METER: 100 attempts to log-in during the lock period after user IP has been locked because of failed log-in attempts of three times

MUST: The locking period should be 15 minutes, and during this period, this IP address can’t be used to log-in any account.

3.5.4 Maintainability

ID: QR16

TITLE: Application extendibility

DESC: The system should be easy to extend. The code should be written in a way that it favors implementation of new functions.

RAT: In order for future functions to be implemented easily.

DEP: none

ID: QR17

TITLE: System testability

DESC: Test environments should be built for the system to allow testing of the system.

RAT: In order to test the system.

DEP: none

3.5.5 Portability Requirements

ID: QR18

TITLE: System portability

DESC: The system should be accessed regardless of operating system, device and Web browser as long as the support for html is valid.

RAT: The adaptable platform to run and access the system.

DEP: none

## Other requirements

ID: QR14

TAG: Personal Privacy

GIST: Privacy of reporter and corresponding patient in the system.

SCALE: The name and other privacy information in the documents should be hidden in some occasions according to the privacy policy.

METER: Check 100 reports with privacy information with account which the information should be hidden from, to see if the privacy protection is active during testing.

MUST: All privacy information is protected.