Software Requirement Specification (SRS) for E-Governence Portal

1. Introduction

1.1 Purpose:

E-Governance Portal is a informative portal of various information is intended to help the citizens of a city/district .

This document is meant to delineate the features of E-Governance Portal, so as to serve as a
guide to the developers on one hand and a software validation document for the
prospective client on the other.

1.2 Scope:

We describe what features are in the scope of the software and what are not in
the scope of the software to be developed.
In Scope:

User can find and able to download the IPC laws, new government schemes, new distribution systems, new or upcoming projects etc.

.
Out of Scope:

Filing the complaint and receiving the response

1.3 Definitions, Acronyms, and Abbreviations:

Acronyms and Abbreviations:
a. E-gov: e- governance Portal
b. SRS: Software Requirements Specification.
c. WWW: World Wide Web.
d. GUI: Graphical User Interface.
e. UML - Unified Modeling Language

f.WWW-world wide web

g.CSS- Cascading Style Sheets

h.IEEE - Institute of Electrical and Electronics Engineers

Accordingly great SRSs will address the following

- Functionality.
- External interfaces.
- Performance.
- Attributes. (the portability, correctness, maintainability, security, etc.)
- Design constraints imposed on an implementation.

According to world standards SRS should be

- Correct
- Unambiguous
- Complete
- Consistent
- Ranked for importance and/or stability
- Verifiable
- Modifiable
- Traceable

If SRS is taken us System Requirement Specifications, it should

- Define the functions of the system
- Define the Hardware / Software Functional Partitioning
- Define the Performance Specification

- Define the Hardware / Software Performance Partitioning
- Define Safety Requirements
- Define the User Interface (A good user's manual is often an overlooked part of the System specification. Many of our customers haven't even considered that this is the right time to write the user's manual.)
- Provide Installation Drawings/Instructions.
- Provide Interface Control Drawings

C. Software Design Document (SDD)

Widely accepted contents of the SDD are:

- Introduction
- Document Outline
- Document Description
- Introduction
- System Overview
- Design Considerations
- Assumptions and Dependencies
- General Constraints
- Goals and Guidelines
- Development Methods
- Architectural Strategies
- System Architecture
- Subsystem Architecture
- Policies and Tactics
- Detailed System Design
- Detailed Subsystem Design
- Glossary
- Bibliography

Design Guidelines for Websites.

User Interface should satisfy the following minimum standards:

- User interface must be simple. This makes system easy to use. The user should be shown only those things that she or he is supposed to see in order to accomplish a task. Special care will be taken in making sure that the user carries out the least number of interactions with application in order to execute a particular function.
- Design must prevent the user from doing something that she/he is not supposed to do. This makes the system more desirable and easy to use. Users will be prevented from performing inappropriate tasks.
- Aesthetics helps in increasing user productivity and the first impression of the web site. The user interface should be aesthetically pleasing.
- In order to have a consistent navigation scheme, system must enable user to access information or perform tasks in same manner and conditions under similar conditions.
- Static text (labels, captions) on the screen must conform to the terminology of the business that the application supports
- Static text (labels, captions) on the screen must follow consistent naming convention, that is same label must convey same meaning at all the places.
- Static text (labels, captions) on the screen must be concise, convincing, and unambiguous
- Use of icons, controls for HTML forms for different purposes like accepting text input, displaying lists, displaying calendars etc. should be consistent across the web site. That is same icon will always mean the same thing, and conversely the same thing should always be represented by the same icon.
- Link to the "Home Page" must be present on all pages.
- User's current location and the navigation path that user followed must be displayed, with hyperlinks on each sub-path, on the screen.
- Display data and information in a format that does not require conversion by the user and is localized to a region.
- Do not use unsolicited graphics and windows "pop-up" to the user.
- Whenever a user leaves the website, the user must be given a feedback clearly telling that the user is moving out of the website.

Home page must have following links

- About Us
- Business tag line that communicates the purpose of web site.
- Contact Us
- Disclaimer

- Feedback
- Login
- Logout
- Site Index
- Site Map
- New changes to web site must be communicated through home page.
- Home page must introduce a user with all the topics on which a web site provides services.
- Low graphic version for home page
- Other available e-Governance applications required to be suitably linked to the site. Dropdown menus may be avoided, if possible, since it would cause difficulty to the aged and physically handicapped users.
- Sufficient interactive pages/applications may be provided on the site for encouraging the usage.
- The portal/ website should follow a well defined Security Policy for Authentication, Access rights, Delegation of Administrative Powers, Password Policy, User Accounts, Validation of content, Identity Management, Server Access Log, Cookies, Transmission Security, Encryption, Auditing, Server Hardening, Terminal Authentication, Terminal logon procedures, User Access Right on Terminals and Database

Security

Firewall Standards: following standards must be ensured while deploying a firewall

- Regular Auditing - This is required to ensure that everything is working in order.
- Logs - Proper logs are to be maintained in order to trace any problems/security breaches, which can occur during normal operations.
- Intrusion Detection- Firewall should be able to detect intrusion attempts.
- Contingency Planning - In case of failure of firewall, there should be plans to recover immediately
- Firewall Access Privileges- Access privileges should be controlled by procedures defined by the organization deploying firewall.

- Disclosure of Internal Network Information- Internal network information must be confidential, proper measures must be taken to ensure confidentiality.
- Posting Updates- If some updates/patches are released for the firewall they must be installed in acceptable time from the release date.
- Monitoring Vulnerabilities- system security should be checked at regular intervals by created false attacks on the system, in order to ensure that system is secure.
- Standard Products- standard products must be used as firewall.

Following measures should be taken for maintaining Physical Security Standards

- Mission critical system facilities must be located in a secure location that is locked and restricted to authorized personnel only.
- Access to "critical" computer hardware, wiring, displays and networks must be controlled by rules of least privilege.
- System configurations (i.e., hardware, wiring, displays and networks) of "critical" systems must be documented. A formal change management process must govern installations and changes to those physical configurations.
- A system of monitoring and auditing physical access to "critical" computer hardware, wiring, displays and networks must be implemented (e.g. badges, cameras, access logs).
- Low and medium risk equipment should be protected by an appropriate alarm system in addition to the correct security enclosures.
- Proper Anti Virus Security Standards

Subsequent updation and maintenance of the sites are the major concern as far as Government Departments are concerned. Generally lethargy is seen in updating the content and analyzing/ responding to the feedbacks being received. These situations required to be changed. As far as major Portals are concerned devoted editorial and development teams should be in place. Periodic Reporting and Periodic monitoring and review by higher authorities are also highly necessary.