Guidelines for Departmental Software Development Proposals

Scope

The following guidelines apply to departmental software design and development proposals for groups managed by the Network Services division of Administration and Finance Information Services. It is recommended that all software proposals include the following elements before being reviewed by the LAN management team.

The purpose of these guidelines is to ensure that software being developed by outside contractors meets the basic industry and UTHSC-H standards for applications systems and that the methodology followed by the contractor provides reasonable assurances that the end users' requirements will be met on time and within budget.

Information Services is ready to assist departments who wish to have outside contractors design and develop departmental systems. Information Services can function as advisors or participate in the project as project managers or provide technical resources as available. Information Services does not recommend that departments with little or no technical expertise attempt to engage contractors to design and develop systems.

Requirements Specification

This section should include a list of processes and functionalities that the finished software package should contain. The use of flowcharts is recommended along with detailed descriptions of the manual and automated process steps.

Descriptions should include detailed information regarding the functionality of the application to be developed. An example would be including sales tax along with the total for an application to be used as a point of sales system. If the system were being used in multiple states it may be necessary to have the sales tax calculated based on the state. This would need to be included ahead of time in the description. A change like sales tax for multiple locations may seem insignificant, but after the application has been developed this would be an expensive and time-consuming change.

If reporting is to be included in the application, the reports should be defined here. The definitions must include the data points to be queried and may also include general layout and appearance requirements.

It is critical that this section contain adequate detail on what the system is supposed to do and how it operates. Since most software proposals contain a change order section, inadequate detail in the requirements specification, means that more change orders will be generated resulting in a significant extra charge and implementation delays. Furthermore, changes made to software after it has been developed can cost 10 – 15 times as much as changes made in the design phase.

Platform Specification

The platform specification should clearly describe the technologies to be utilized. Proposals should include the programming language and development tools to be utilized on both the client and any back-end systems. The application should be written using Microsoft technologies, Java, or JavaScript.

A description of the minimum and recommended hardware specifications should be included with associated performance expectations. It should be specified whether other applications can reside on the same system or whether this software requires dedicated hardware. The number of users supported should be listed for both the minimum and recommended hardware specifications. The software should work on Intel based Compaq (HP) hardware.

The software should be compatible with all current desktop operating systems in production in our enterprise, with currently released updates and security fixes. The back-end application should meet this same requirement for server operating systems and applications.

If additional software is required by the application it should be specified here as well. The additional software must meet the same requirements as the application that is being developed.

Security

When requesting customized software, keep in mind that every enterprise has unique security requirements. IT security includes:

- Network security,
- Server security and
- Application security.

Network security is handled by the university IT infrastructure owners but can affect the design and implementation of the application being proposed. For example, the security needs of the application may require it to be behind the firewall. If so, the specific protocols and ports required should be clearly defined.

Server security is handled by the server administrator, in this case, Network Services. For applications that contain sensitive personal or financial data additional security functionality will be required. Communication on these systems should be secured using SSL, SSH, IPSec, or another industry standard encryption protocol. Proprietary encryption protocols are not sufficient and will require an industry standard protocol to ensure security.

Application security is designed and developed by the contractor and must protect the data contained in the system from accidental or deliberate misuse by application users. Depending on the specific application, a description of the different levels of authorization \ access should be included. These should be detailed descriptions that clearly define the functional roles. This is typically defined by describing access levels as view, add, change, or delete by field, record, database or transaction type. System security must be commensurate with the confidentiality or sensitivity of the data.

It may also be necessary to include provisions for user tracking and auditing. Authentication should be done through Active Directory, digital certificates, or LDAP (v3 compliant). Authentication through LDAP is highly recommended since this directory is updated automatically through PeopleSoft relieving the application administrator of this task. SQL Authentication is acceptable but strongly discouraged. If application level security is to be utilized, usernames should correspond with the user's UID from the Netscape Directory server and passwords should meet the University's password policies. The software should provide a utility to force password expiration.

Applications that use confidential data downloaded from another application must maintain the same level of security as the original system. The system owner and the system custodian must take responsibility for the security of the application and server. They must sign a Memorandum of Understanding describing their role in securing and maintaining the data.

The extent of security will depend on the application and the data that it utilizes. Please contact your LAN management team or the IT Security department for further details and requirements.

Coding Standards

All applications should follow generally accepted good coding practices. These recommendations can usually be found on the manufacturer's website.

The final production source code for the application should be provided along with a data flow diagram. In addition, if a database is being utilized, an entity relationship diagram and \ or database schema diagram should be included.

General specifications include the following:

All source code should be clearly commented

Error trapping routines should be present for each procedure so that in the event of failure, the software will fail gracefully

All procedures, loops, and conditional statements should be indented to provide for legibility in the code

"Shorthand" notation should never be used

Variable declarations should be consistent

Single line conditional statements should not be used. Instead use a code block.

All forms should have proper conditional formatting and error checking.

Backups \ Disaster Recovery

Clear instructions on backups of the data store should be provided including any regular maintenance that should be performed on the system. The maintenance schedule should also include the role of the person to perform the maintenance as defined in the security specification.

Applications utilizing a database should provide a utility for archiving data and purging the records from the database. The frequency with which this is performed will be dependant on the specific application.

Documentation

Both technical and user documentation should be provided. All documentation should be provided at final delivery of the product or before. In addition to this documentation, a list of all system and core files that may be changed and application specific registry entries should be included as well.

Technical Documentation

This documentation should include detailed installation instructions for both the client side and back-end system (if applicable.) The documentation should include screenshots of the installation at various stages so that it is easy to follow. This documentation should be provided in electronic format as well as a hard copy.

User Documentation

This documentation should include detailed descriptions of how to perform the various processes outlined in the requirements documentation. The roles of the users to perform the processes, as defined in the security documentation, should be listed for each procedure. Screenshots of various stages of the process should be included for clarity.

Testing Standards

It is essential that the proposed testing plan include an opportunity for both the application user and the LAN management team to test and <u>accept</u> the system. After an application has been developed there will be a minimum two-week testing phase by the LAN management team to ensure that the software is safe for production machines. During this time, the department may also review the software for the functional requirements. The LAN management team does not review the software for the functional requirements only for security and operability in our enterprise. Functional testing is the responsibility of the application owner (user) and is a time consuming task that must be taken seriously because it represents the final signoff of the application after which the user will be charged for changes.

Project Plan

A multi-phase project plan should be provided. The project plan should include:

- Requirements definition,
- System design
  - Functional
  - Technical
- Development
- Testing
  - Unit
  - System
  - Acceptance test
    - Functional
    - Technical
- Implementation
  - Conversion
  - Training
  - Installation at UT-H

An appropriate number of signoffs should be included to ensure that satisfactory progress is being made and that the requirements are being met. After the design phase there must be an initial review for functional requirements. Should the functional requirements not be met, we should retain the right to back out of the project with no further financial obligation. Once the design has been approved, further work can continue.

The pricing structure should be broken down to reflect this as well. All charges should be broken down to show hourly rates and how many hours for each phase of the project. Payment amounts and times should be clearly defined.

There should be provisions for technical and functional walkthrough discussions throughout the project at either party's request.

Team Members

The following team members should be identified prior to the proposal being approved:

Functional Representative

This person is responsible for compiling the requirements specification. They should be intimately familiar with the processes for which the software will be developed.

Technical Representative

This person should be a member of the LAN management team. They should have a clear understanding of the technologies being proposed for utilization.

Internal Project Manager

This person is responsible for communicating with the vendor. They are also responsible for scheduling periodic status meetings and ensuring that the project time line is adhered to.

Security Representative

This person is optional but should be included for any applications that could potentially have components that would reside in a secured network zone. They are responsible for ensuring that the application meets the University's security requirements.

Vendor Project Manager

This person will be the single point of contact for all questions from the internal team. They should work closely with the Internal Project Manager to insure that the customers' expectations are being met.