

**iStar System  
Policies and Procedures**

**Version Number: 1.0**

**Date Issued: March 7, 2007**

**University of Southern California Health Sciences Institutional Review Board  
University of Southern California University Park Institutional Review Board  
Childrens Hospital Los Angeles Committee on Clinical Investigation**

## Table of Contents

	<b>Page Number</b>
<b>1. List of Abbreviations.....</b>	<b>3</b>
<b>2. Introduction.....</b>	<b>4</b>
2.1 Overview of iStar System.....	4
2.2 Purpose and Applicability.....	4
<b>3. iStar User Information.....</b>	<b>5</b>
3.1 General Information about the User Interface.....	5
3.1.1 Personal Folder.....	5
3.1.2 Study Workspace.....	5
3.2 iStar User Procedures.....	5
3.2.1 PI&Staff.....	5
3.2.2 Pre-Reviewer.....	6
3.2.3 Committee Member.....	6
3.2.4 IRB Administrator.....	7
3.2.5 IRB Director.....	8
3.2.6 IRB Chair.....	8
3.2.7 Ancillary Committees.....	9
3.2.8 iStar Help Desk.....	9
3.2.9 iStar Account Manager.....	9
3.2.10 iStar Site Manager.....	9
3.2.11 References.....	9
<b>4. iStar Technical Information.....</b>	<b>10</b>
4.1 User Account Verification.....	10
4.2 User Account Creation and Maintenance.....	10
4.3 Password Policy.....	11
4.4 User Authentication.....	11
4.5 Protocol Modification and Audit Trail.....	12
4.6 iStar System Equipment.....	12
4.7 System Validation.....	13
4.8 System Version Increments.....	14
4.9 Upgrade Patch Installation.....	14
4.10 Server Log Maintenance.....	16
4.11 Process Flow Management and Development Process ...	16
4.12 Backup and Disaster Recovery Procedures.....	17
<b>5. Standard Operating Procedures and Maintenance.....</b>	<b>19</b>
5.1 Review, Revision, and Approval of SOPs.....	19
5.2 SOP Dissemination and Training.....	19
5.3 Responsibility.....	19
5.4 Applicable Regulations and Guidelines.....	19

## **1. List of Abbreviations**

CCI	Committee on Clinical Investigation (Childrens Hospital Los Angeles)
CHLA	Childrens Hospital Los Angeles
CIC	Clinical Investigations Committee (Norris Comprehensive Cancer Center)
DHHS	Department of Health and Human Services
FDA	Food and Drug Administration
HSIRB	Health Sciences Institutional Review Board
IIS	Internet Information Services
IRB	Institutional Review Board
iStar	IRB Submission Tracking and Review
OHRP	Office for Human Research Protections
PI	Principal Investigator
UPIRB	University Park Institutional Review Board
USC	University of Southern California

## **2. Introduction**

### **2.1 Overview of iStar System**

iStar (IRB Submission Tracking and Review) is an Internet-based software application for the submission and review of research projects involving human subjects. iStar is a collaboration between the Institutional Review Boards (IRBs) at the University of Southern California (USC) Health Sciences Campus, the USC University Park campus, and the Committee on Clinical Investigation (CCI) at Childrens Hospital Los Angeles (CHLA). CCI is the Institutional Review Board of Childrens Hospital Los Angeles.

iStar was developed in conjunction with Click Commerce and implemented at USC and CHLA in 2004. iStar was developed with the goals of standardizing and computerizing the submission of research projects, improving the efficiency of the submission and review process, and better ensuring the protection of research participants.

### **2.2 Purpose and Applicability**

The purpose of the iStar System Policies and Procedures is:

- To provide an overview of the iStar electronic submission system
- To serve as a reference guide for iStar users and iStar staff
- To document that the electronic iStar review and approval process is generally equivalent to paper records and handwritten signatures
- To demonstrate iStar compliance with federal regulations for study sponsors, the participating institutions, and FDA, HHS, OHRP, and other regulatory agencies

The iStar Policies and Procedures apply to the iStar staff, IRB Chairs and IRB staff members at USC and CHLA. The Policies and Procedures are available to all iStar users on the iStar web site (<https://istar-chla.usc.edu>).

### **3. iStar User Information**

#### **3.1 General Information about the User Interface**

##### **3.1.1 Personal Folder**

Once users log in to iStar, their Personal Folder appears. The Personal Folder is the central resource for managing study applications and is customized to the selected user role. The Personal Folder provides users with all the tools they need to fulfill their roles in iStar. Individuals who have more than one user role select the user role for the study they want to view and the corresponding Personal Folder opens.

The Personal Folder displays the following selections:

- My Inbox Tab – displays all studies that require some task to be done by the user or study team.
- Studies, Reportable Events, Amendments, and Continuing Reviews Tabs – display all studies the user is a part of, regardless of where a study is in the submission and review process.

##### **3.1.2 Study Workspace**

Clicking on the name of a study in the Personal Folder opens up the workspace for that study. The workspace lists all activities available to the user and provides access to the SmartForms, approval documents, study history, and other study information.

#### **3.2 iStar User Procedures**

##### **3.2.1 PI&Staff**

Principal Investigators (PI), co-investigators, study coordinators, and study staff prepare and submit new studies, amendments, reportable events, and continuing reviews to the IRB. Study staff given “Edit Permission” may read and edit the study application. Study staff given “Read Permission” may read, but not create or edit, study applications. All study staff may read correspondence between the IRB and the study team. The PI and co-investigators are the only members of the study staff who can submit reportable events to the IRB.

Study staff with permission to edit a study may submit study amendments, continuing review forms, and responses to IRB contingencies. The general submission procedures include:

- Log in with user name and password
- Navigate to study workspace
- Complete new form or edit existing form
- Attach revised study documents to application
- Submit to IRB

The PI is the only member of the study staff who can submit new applications to the IRB. Additional activities required to create and submit new applications include:

- Obtain co-investigators' agreement to take part in the study.  
Co-investigators must indicate their agreement to participate in the study by completing the "Agree to Participate in Study" activity. Co-investigators agree with the policies and statements shown on the activity screen by completing the checkbox on the screen and clicking "OK." The date, time, and user's name are recorded in the history log as an electronic signature. Co-investigators who do not agree to participate must be removed from the study before it can be submitted to the IRB.
- Agree with Investigator's Assurance.  
The PI must indicate agreement with the Principal Investigator's Assurance before the study can be submitted to the IRB. PIs who are trainees or students must also indicate their agreement to the Trainee/Student Investigator's Assurance. PIs agree with the policies and statements shown on the activity screen by completing the checkbox on the screen and clicking "OK." The date, time, and user's name are recorded in the history log as an electronic signature.
- Obtain required organizational approvals from department, division, or school pre-reviewers.  
Pre-reviewers must complete the "Approve Protocol" activity before the study can be submitted to the IRB. Pre-reviewers agree with the policies and statements shown on the activity screen by completing the checkbox on the screen and clicking "OK." The date, time, and user's name are recorded in the history log as an electronic signature.

### **3.2.2 Pre-Reviewer**

Pre-Reviewers review and approve studies on behalf of their department, division, school, or organization before the studies are submitted to the IRB. Pre-Reviewers include Faculty Advisors, School Deans, Department Heads, Division Chiefs, and the Clinical Investigations Committee as designated by the institution.

The Pre-Reviewer receives an e-mail notification that a study requires review. The Pre-Reviewer logs in to iStar and reviews the study application and attached documents. The Pre-Reviewer chooses one of two activities:

- Division/Department Review Approve Protocol – this activity records approval of the study for the specific division, department, or school the user is allowed to approve for.
- Division/Department Reviewer Request Changes – this activity sends the study back to the study team for the changes indicated by the reviewer. The study team is notified of the requested changes.

### **3.2.3 Committee Member**

Committee Members are members of one or more of the IRBs. Committee Members review new submissions, study amendments, continuing reviews, and reportable events that require full committee review and record their reviews in iStar. Committee Members may view only the studies assigned to be reviewed by the IRB(s) of which they are a member.

Committee Members receive an e-mail notice when they are assigned a study to review. The Committee Member logs in to iStar and, if necessary, selects the Committee Member user role. The Committee Member reviews the new or revised application and study documents.

To record the review, the Committee Member:

- Types comments and questions directly into the comments text box or attaches an MS Word document containing the comments and questions.
- Adds edited study document(s) if applicable.

### **3.2.4 IRB Administrator**

IRB Administrators are the IRB staff members who have ownership of the study and perform IRB staff actions on the study. The IRB Administrator for a given study is the IRB contact person for investigators and study staff and for committee members reviewing the study. All IRB Administrators at a particular campus can open and view all studies at that campus; however, only the IRB Administrator of record may perform administrative actions on the study.

iStar has general procedures in place for administering IRB submissions. Each campus may have additional, specific procedures designed to meet the needs of the IRB staff at that campus. In general, the IRB Administrator performs the following activities:

- Take ownership of a study.  
New studies are either: (1) assigned to the IRB Administrator by the IRB Director or (2) the IRB Administrator takes ownership of an unclaimed study under the "Shared Queue" tab that appears in the personal folder of each IRB Administrator. If necessary, a different IRB Administrator may take ownership of a study.
- Process a full committee study (new studies, modified studies, or continuing reviews).  
The IRB Administrator reviews the study and records the staff review, assigns the study to an IRB committee, and assigns the study to a meeting agenda.
- Record meeting results and generate IRB letter.  
The IRB Administrator records the results of the meeting, which includes the committee's discussion, contingencies, action, and vote. The IRB administrator sends the recorded results to the IRB Chair for confirmation. The Chair either confirms the results or requests changes and returns the study to the IRB Administrator. If the Chair confirms the results, the IRB Administrator generates the action letter from the confirmed minutes and sends the letter to the study staff. If the Chair requests changes, the IRB Administrator makes the requested changes and returns the study to the Chair for confirmation. iStar does not permit the IRB Administrator to send the action letter to the PI until the Chair has confirmed the results of the meeting.
- Process an expedited or exempt study.  
The IRB Administrator reviews the study, records the staff review, and forwards the study to the designated expedited-exempt reviewer. The expedited-exempt reviewer reviews the study, determines the action, specifies any contingencies, and returns the study to the IRB Administrator. The IRB Administrator generates the action letter and sends the letter to the study staff. iStar does not permit the IRB Administrator to send an action letter to the PI until the expedited-exempt reviewer has decided upon and recorded the appropriate action.

- Process submitted contingencies.  
The IRB Administrator reviews the PI's response to contingencies and forwards the study, along with any comments regarding the staff review, to the designated reviewer. The designated reviewer reviews the study, determines the action, and returns the study to the IRB Administrator. The IRB Administrator generates the action letter and sends the letter to the study staff. iStar does not permit the IRB Administrator to send an action letter to the PI until the designated reviewer has decided upon and recorded the appropriate action.
- Stamp approved informed consent documents.  
The IRB Administrator finalizes the informed consent document approved by the full committee or designated reviewer. The IRB Administrator pastes the blank IRB approval stamp into the approved document, verifies the approval and expiration dates, adds the document to the study, and, if necessary, selects the previously approved document that it will replace. iStar automatically fills in the date fields in the stamp and moves the documents to the approved consent section of the study workspace. All finalized documents are permanently locked so no further editing is allowed. An unlocked version of the document without the stamp is provided to the study team to use for any future modifications.

### **3.2.5 IRB Director**

IRB Directors at each campus assign new studies to IRB Administrators and reassign studies among IRB Administrators as needed to manage the work flow. IRB Directors also have the role of IRB Administrator and can perform any IRB Administrator function. IRB Directors receive an email notification when a new study arrives at the IRB or when an existing study remains in the inbox of an Administrator or Chair longer than the designated review time frame.

Each campus may have additional, specific procedures designed to meet the needs of the IRB Staff and Committee Members at that campus. In general, the IRB Directors perform the following activities:

- Assign new submissions, including full committee and expedited-exempt studies, to IRB Administrators.
- Take ownership of a study from an IRB Administrator or reassign ownership of existing studies among IRB Administrators as needed to manage the work flow and cover vacation periods.
- Perform any function of an IRB Administrator.
- Review studies submitted under the Facilitated Review process and forward them to the IRB Chair for review and approval.

### **3.2.6 IRB Chair**

IRB Chairs at each campus review and decide the appropriate action for new and continuing studies that are eligible for expedited, exempt, facilitated, coded specimens/data, not engaged, or administrative review. IRB Chairs also review and confirm the minutes for studies that were reviewed by the full committee.

The IRB Chair receives an e-mail notice when there is a study to review. The IRB Chair logs in to iStar and, if necessary, selects the IRB Chair user role. If the study has not been assigned to a specific Chair, the IRB Chair must claim the study before submitting the chair review. The IRB Chair reviews the study, records the Chair review, and returns the study to the IRB Administrator who owns the study. The IRB Chair performs the following activities:

- Review new studies that are eligible for expedited or exempt review.
- Review modified studies that are eligible for expedited review.
- Review continuing review applications that are eligible for expedited review.
- Review reportable events that meet the criteria for review by the IRB Chair.
- Review and confirm the minutes for studies that were reviewed by the full committee.

Each review submitted by an IRB Chair is logged in the history log with the date, time, and IRB Chair's name. By checking the "I'm done with this review" checkbox and clicking OK, the IRB Chair is electronically signing the submitted review.

### **3.2.7 Ancillary Committees**

Ancillary Committee members are given read-only permission for studies that meet specific criteria. The Ancillary Committees include Health Research Association (HRA), General Clinical Research Center (GCRC), USC Contracts and Grants, the Pathology Department at LAC+USC Medical Center, and various committees at CHLA.

### **3.2.8 iStar Help Desk**

The iStar Help Desk answers questions from users. The Help Desk is a user role that allows Help Desk staff to view studies from all three institutions. The iStar Help Desk user can view all items in the history log for the study.

### **3.2.9 iStar Account Manager**

The iStar Account Manager creates and edits accounts for users. The Account Manager can edit contact information, edit user roles, and reset passwords. The Account Manager role is limited and the Account Manager cannot access any user passwords.

### **3.2.10 iStar Site Manager**

The iStar Site Manager can play all other user roles and has global edit permissions. The Site Manager can directly edit a study, amendment, continuing review, or reportable event, but that action is not recorded in the history log. The Site Manager is required to document any edits using the "Log Comment" or "Send Message to Investigator" activities.

### **3.2.11 References**

For additional information or detailed procedures, please refer to the following:

- iStar Instructional "Quick Sheets"
- iStar User Guide for Investigators and Study Personnel
- Guidance for each item in the iStar SmartForm
- IRB External Adverse Event Reporting Policy

## **4. iStar Technical Information**

### **4.1 User Account Verification**

iStar has two levels of personal profiles recorded in the system. The first is a contact profile that allows recording of name, organization, email address, and certification information. A contact profile is required before a user account can be created. In addition, contact profiles are created without a user account if there is a need to track certification information such as completion of human subjects protection education but the individual has no need to access iStar. These contact profiles are not verified when created.

The second level of the personal profile is the user account. A user account is needed to access any confidential information in iStar. A user account is not necessarily verified upon creation, but is verified before a study containing the user account is approved. The methods of verification are:

- User accounts with email addresses in the usc.edu and chla.usc.edu domains are automatically verified by the fact that they have email address in those specified domains. USC and CHLA have verification policies in place before they will grant an email address in their domains.
- User accounts for the PI&Staff user role (default user role) with email addresses outside the usc.edu and chla.usc.edu domains are not verified until they are listed as part of the study personnel on an IRB application. The verification is the responsibility of those individuals adding the new user account to the study application and submitting it to the IRB.
- User accounts for other user roles, such as Committee Members who have outside email addresses, are verified by the IRB Director, IRB Administrator, or Account Manager before the user account is created.

### **4.2 User Account Creation and Maintenance**

iStar user accounts are created for individuals who conduct research requiring review by the CCI, HSIRB, or UPIRB. New users request an iStar user account by sending an email message to [istar@usc.edu](mailto:istar@usc.edu) or by phoning the iStar Help Desk. An account request can be made on behalf of someone as long as that individual is aware the request is being made. Basic information (the user's name, organization, and email address) is required to create the iStar account and for account maintenance and function. Users provide additional contact information later by editing their iStar profile. Once the basic information is entered, an iStar account with a unique username is created for the requestor. Generally, the username is the first part of the provided email address if the email is from [chla.usc.edu](mailto:chla.usc.edu) or [usc.edu](mailto:usc.edu); otherwise, the username is the entire email address. Occasionally, due to uniqueness constraints or long email addresses, the iStar username is a modified version of the email address.

All general iStar accounts are given the user roles of Registered User, which allows login to iStar, and PI&Staff, which allows submission of study materials to the IRB. A personal folder, allowing easy access to the user's materials based on user role, is assigned to the

account. The user is notified of the account creation and the account information by an email notification sent to the email address provided in the request. This notification contains the user's email address, a temporary keyword, and the link to the iStar site. It also contains contact information for help with iStar if there are any problems with the account.

Users authenticate themselves with the iStar site the first time they access iStar. The user must supply the username and temporary keyword supplied in the email. The system will then prompt the user to change the keyword to a password known only to the user. Subsequent login sessions will use the assigned username and the new password created by the user.

Users can request password changes by one of three methods: (1) clicking the "Forgot Password?" link under the login component and supplying the required information, (2) calling the iStar Help Desk and providing their name and iStar username, or (3) emailing [istar@usc.edu](mailto:istar@usc.edu) with their name and username indicating their request to change their password. Any of these methods will result in an email notification being sent to the email address on file with a new temporary keyword. The temporary keyword will work as the password and will then require the user to change the password to something known only to the user. Account passwords are encrypted on the server and are not accessible by any iStar or server account.

An account may be disabled, which means the user is not allowed access to iStar resources, under the following conditions: (1) the individual has left the institution and no longer participates in research reviewed by the IRB, (2) the user account has tried unsuccessfully to login 10 times and account is disabled automatically, and (3) prohibited account behavior has been reported to the iStar team and reviewed by the iStar Site Manager.

### **4.3 Password Policy**

iStar requires every user to have a password known only to the user. The password must be at least 4 characters (letters, numbers, or symbols) and does not expire. A new password does not have to be different from a previous password.

The user's password must remain confidential. If there is any suspicion that a password has been compromised, the user must change the password using one of the three methods described above. Any sharing of passwords is strictly prohibited. Any unauthorized use of a password should be reported to the iStar Help Desk. Unauthorized use of an iStar account or the iStar system may lead to termination of the session and subject the user to disciplinary action as well as civil and criminal penalties.

### **4.4 User Authentication**

To access any confidential or secured material on the iStar system, the user must have a secured token registered with the system. The user obtains a secured token by submitting the username and password over SSL, which encrypts the information exchange. If the username and password match an active account on the iStar system, a secure token is created on the client machine. Each time the user accesses a resource on the server, the server checks that the

user has a secure token and checks if the user indicated in the token can access the resources. If either of these does not match, the user is shown the “permission denied” page. The secure token is unregistered with the server if (1) the user logs off, (2) the user is inactive for 60 minutes and the token expires, or (3) the browser instance is closed, thereby destroying the token.

#### **4.5 Protocol Modification and Audit Trail**

For all users except Site Managers, any modification or action performed on a study, amendment, continuing review, or reportable event is recorded in the history log with the date, the time, the name of the user making the change, and the properties that are changed. If the activity includes an activity screen (for example, Expedited Review) a snap shot of the activity screen is recorded in the activity details. If a system event changes a study (for example, automatic expiration), this is recorded in the same manner in the history log.

Because the Site Manager has global edit permissions, the Site Manager can directly edit a study, amendment, continuing review, or reportable event without the modification being recorded in the history log. If this occurs, the Site Manager is required to document what was changed via the “Log Comment” or “Send Message to Investigator” activities. These activities then appear in the history log with the date, time, user name, and description of the change.

The study workspace and history log for each study provide a secure audit trail. The iStar system independently records the time and date of user activity and does not obscure previously recorded information. iStar users cannot modify the audit trail.

#### **4.6 iStar System Equipment**

The iStar system is designed to work in a 4 server environment. The specifications for each server are decided by the iStar Site Manager with consideration to function and projections of use. The server roles are:

1. **Production Server.** The production server functions as the main iStar server. All data contained on the production server is current. The domain name `istar-ch1a.usc.edu` is mapped to the IP address of this server. iStar users only access this server. Any system issue identified with the production server is considered critical. The production server specifications are required to meet or exceed the projected usage patterns of iStar system use in respect to processor speed, memory, and hard drive space. The production server is backed up to tape nightly, in addition to the 30 minute data transfers to the hot-spare server.
2. **Hot-spare Server.** The hot-spare server functions as a backup and disaster recovery server. Data is shipped from the production server to the hot-spare server on half hour intervals. The data on this server may be up to 30 minutes old. iStar users do not have access to this server and the IP address is inaccessible from the internet. Any system issue with the hot-spare server is considered high priority because of the backup and disaster recovery function. The hot-spare server specifications are identical to the production server. The hot-spare server is not backed up to tape. In the event of a

disaster to the production server, the iStar Site Manager or server administrators will perform the iStar Disaster Recovery Plan, thereby taking the production server offline, and making the hot-spare server the new production server. Any Extranet base product upgrade using its own installer must also be separately applied to the hot-spare server. Any upgrade installed using the Webridge Administration Manager is not required to be installed on the hot-spare server since the upgrade will automatically be installed with the next data transfer from the production server.

3. **Staging Server.** The staging server should be similar to the production server in specification, but variations can be allowed since the function of this server is limited. The function of the staging server is to provide a replicated environment of the production server to test installation of any iStar patches or server configuration changes. Before testing a patch or configuration change, the staging server must be loaded with the most recent backup from the production server. This will allow the staging server to have data not more than 24 hours old. All patches and configuration changes are tested on this server and must be successful before they can be applied to the production and hot-spare servers. The staging server is not required to have any backup strategy.
4. **Development Server.** The development server should be similar to the production server in specification, but large variations can be allowed since the usage of this server is limited to iStar and Click Commerce developers. All changes to configuration are performed and tested on the development server. Changes to configuration are under source control. Any configuration item must be checked out of source control before changes can be made. Once the changes are complete, the configuration item is checked back into source control. Source control records a history of each item and the changes made. The development server is backed up to tape nightly to retain the record of source control changes and current development work.

#### **4.7 System Validation**

Initial system validation was performed by the iStar development group during the alpha and beta testing phases. Subsequent system validation is performed on a staging server when upgrades are applied to the system. The following validation schemes are used depending on the version increment of the upgrade.

- **Major version increment (x.x) - full system validation.** Testing procedures are used to exercise all project workflows, activities, and data entry screens by user roles. In addition, account maintenance is tested. Incorrect results are recorded on preprinted state transition diagrams and application screenshots. These testing worksheets are signed by the tester and submitted to the iStar Site Manager for review and archival in the system validation binder.
- **Minor version increment (x.x.y) – unit testing only.** Testing procedures are performed on all changed items in the patch as well as areas that may be affected by the changes. Each issue addressed in the patch has a detailed test plan to unit test the change and affected areas. The test plans are consolidated and preprinted for the testers. These testing worksheets are signed by the tester and submitted to the iStar Site Manager for review and archival in the system validation binder.

## 4.8 System Version Increments

There are three levels of system upgrades, two of which will increase the system version number. The system version number takes the format x.x.y and has the following increments:

- Major increment (x.x). The major version number is based off of the Click Commerce base product version number. The first part of the number is incremented whenever the base product is upgraded by a major version number. The second part of the number is incremented whenever the base product is upgraded by a service pack.
- Minor increment (x.x.y). The minor version number is based off the customized patches applied specifically to the iStar system and is assigned sequentially. The minor version number is the third part of the iStar version number. Minor version numbers above 10 are possible if there are more than 10 customized upgrades applied to the iStar system between base product service packs.
- Hotfix. Hotfixes to production do not increment the iStar version number, but are recorded system version information maintained by the iStar Site Manager. Hotfixes address specific issues that cause blockages in iStar workflows or system errors affecting multiple users that cannot wait until the next customized upgrade. Hotfixes are tested in a staging environment before being applied to production.

**Example:** If the current iStar version is 1.6.2 and the Click Commerce base product is upgraded from version 5.5 to 6.0 (a major base product upgrade), the new iStar version will be 2.0. If the current iStar version is 1.6.2 and the Click Commerce base product is upgraded by a service pack for version 5.5 (a minor base product upgrade), the new iStar version will be 1.7. If the current iStar version is 1.6.2 and there is a new custom upgrade to the iStar system (a minor increment), the new iStar version will be 1.6.3. If the current iStar version is 1.6.2 and a hotfix is applied, the iStar version number will remain 1.6.2 since hotfixes do not change the iStar version number.

## 4.9 Upgrade Patch Installation

The dates of each step are calculated backward beginning with the targeted date for the upgrade patch to be applied to the iStar server. Patch installations are performed in the following steps:

1. Code Cutoff. The code cutoff deadline is the date at which no new enhancements will be included in the upcoming patch upgrade. Adjustments to the code for enhancements already included will be allowed if issues are identified during the testing phase.
2. Unit Testing of Changed Items. Each support case marked “fix to be verified” for the current patch number has a unit test plan. The test plans are consolidated and tested. Any issues are marked on the test plan and forwarded to the iStar Site Manager. Issues may or not be addressed before the next step if this upgrade is a major version change. If it is a minor version change, all issues must be addressed.
3. Full System Testing. Full system testing is required for major version changes where the base product has been upgraded. A master test plan will be created and issued to testers. The testers will identify any issues to the iStar Site Manager. All issues must be addressed before moving to the next step.

4. Patch Creation. The upgrade patch file is created using Extranet's Process Studio. The system compares the previous label (associated with the last update applied to the iStar system) with the current label in source control. All items changed and checked in between the two labels are included in the patch file. The patch file name is iStar.x.x.y.zip where x.x is the major version number and y is the minor version number.
5. Test Installation on Staging Server. The patch file is transferred to a staging server where it is installed on the latest recreation of the iStar site (normally the previous night's backup). The beginning and ending times for the installation are recorded to accurately plan the size of the upgrade window. The application log is monitored for errors. If the patch installation fails, the application log is analyzed to determine the source of the failure. If the failure is due to missing items in the patch file, the upgrade patch will need to be recreated on the development server.
6. Full System or Unit Testing on Staging. Once the upgrade patch is successfully installed on the staging server, full system testing or unit testing is performed. The same test plans used in steps 2 and 3 are used. Any issues arising on the staging server with current data are recorded and forwarded to the iStar Site Manager. Significant issues may require returning to step 1 for code fixes and recreation of the upgrade patch.
7. Notification of Upgrade to All iStar Users. Once staging is complete, a system notice will be posted on the iStar site to notify users of the planned upgrade. The upgrade window will be based on the time needed to install on the staging server (step 5) plus any additional time needed to perform post-installation configuration and system status verification. Public notice is required to be posted in the following methods:
  - Alert notice posted on the front page of the iStar system
  - Alert notice posted on the system status page of iStar
  - Single line alert with link to system status page posted on all personal folder templates
  - Email notification to all active iStar users with the "Send System-Wide Notification" activity
  - The new version information is required to be posted in the system information section of the iStar site. A link to the new version information should be included in any alert notice or email notification about the upgrade.
8. Scheduled Installation on Production Server. Prior to the installation window, a full backup of the iStar system is required and is transferred to the hot-spare server. Sequential transaction logs after the full backup are also sent to the hot-spare server. This process is automated, but must be confirmed before the installation can take place. The installation on the production server has the following steps:
  - a. Redirection of IIS homepage to the iStar maintenance page
  - b. Addition of the iStar testing virtual root at /istarx
  - c. Removal of the iStar main virtual root of /istar
  - d. Creation of a test study prior to the patch upgrade
  - e. Recording of counts of contact, organization, and all project types; the project counts are obtained using the "Project Counts" script in the debug console
  - f. Upgrading patch installation using the Webridge Administration Manager or base product patch file

- g. Accessing iStar site after successful patch installation via the testing virtual root and all contact, organization, and project types are verified
- h. Post-installation configuration (if necessary)
- i. Restoration of iStar main virtual root of /istar
- j. Removal of iStar testing virtual root of /istarx
- k. Restoration of the IIS homepage redirection to the /istar virtual root
- l. Updating of iStar system version on the front page of the site to the new version number
- m. Updating of all alert notices on the iStar system to indicate completion of the scheduled upgrade and link to the new version information.

#### **4.10 Server Log Maintenance**

Monthly maintenance of the logs on the server is required to archive the logs and conserve space. The sets of logs that are archived are the logs necessary to track system access and processing. The log sets are (1) Extranet application logs, (2) IIS web logs, and (3) IIS SMTP logs for email.

At the beginning of each month, the log files from the month before last are zipped into an archival folder and stored in the “old logs” directory. For example, at the beginning of October the August logs will be archived. The archived log files are kept for a minimum of two years. The file name for the archived logs is “logs.YYYY.MM.zip,” where YYYY is the four-digit year and MM is the month.

The logs are zipped from the following folders with full path information:

- E:\Logs\Extranet
- E:\Logs\IIS-Services\W3SVC1
- E:\Logs\IIS-Services\SMTPSVC1

Logs are maintained as individual files for the first month. At the beginning of the second full month, log files are transferred to a zip archive and kept for a remaining two years.

#### **4.11 Process Flow Management and Development Process**

iStar is a state transition machine incorporating a set of project states and a set of rules governing transition from one state to the next. Process Flow Management is a method for defining and managing the flow of the submission and review process across three separate institutions. Appropriate individuals at each of the institutions (i.e. working group) must agree to changes or enhancements involving the iStar process.

Each individual enhancement or issue is tracked individually with the support case system in iStar. The steps in the process are:

1. Initial Request. An enhancement request or support case may be started by any iStar user. If the user has access to the iStar support case system, the user may proceed directly to step 2. If the user does not have access to the iStar support case system, the user may contact the iStar Help Desk.

2. **Support Case Submission.** A new support case is created in the iStar support case system with information describing: (1) the enhancement or issue, (2) priority, (3) areas of the system affected, and (4) steps for recreation. In addition, supporting documentation may be included.
3. **Issue Resolution.** If the support case indicates an issue not involving changes to the iStar system, the issue is resolved by the iStar Help Desk or escalated to a developer for assistance. Upon satisfactory resolution of the issue, the support case is closed out.
4. **Working Group Discussion.** If the support case indicates issues that will cause changes to any study applications or workflow configurations, the issue is discussed with the iStar working group at a regularly scheduled meeting
5. **Working Group Signoff on Paper.** All changes to application questions, SmartForm path, and workflow are documented on paper and distributed to the working group. Each IRB must sign off the proposed changes before development can begin.
6. **Checkout of Items on Development.** Items affected in the issue configuration are checked out of source control on the development server.
7. **Development Configuration.** The proposed changes are configured on the development server.
8. **Unit Testing on Development.** Once configuration is done, the iStar developer will test the changes to ensure they work as proposed by the working group.
9. **Unit Testing by Working Group.** Working group members will be allowed access to the development server to test the proposed enhancement or issue. If instructions are necessary, they will be provided by an iStar developer.
10. **Working Group Signoff.** Each IRB must sign off on the overall enhancement as configured on the development server before the items can be checked in and included in the next upgrade patch.
11. **Check-in of Items on Development.** After group signoff, all configuration items changed will be checked back into source control. The check-in comments will include a summary of changes and the support case number describing this enhancement or issue.
12. **Fix Recorded in Support Case.** The support case is marked "Fix to be Verified" and a unit test plan is recorded.
13. **Fix Verified in Patch.** Prior to upgrade patch creation, the fix is verified using the test plan provided in the support case. The fix is again tested when the patch is applied to the staging server.
14. **Support Case Closeout.** Upon patch installation in the iStar system, satisfactory resolution is confirmed from the initial submitters of the request and the support case is closed out.

#### **4.12 Backup and Disaster Recovery Procedures**

The backup schedule for each of the iStar servers is determined by the server function and controlled by the iStar Site Manager. The iStar Disaster Recovery Plan is maintained as a separate document and is the responsibility of the iStar Site Manager. The plan is periodically revised to address changes to backup strategy, server configurations, or contact information. A current copy of the iStar Disaster Recovery Plan must be distributed to the following individuals/locations:

- iStar Site Manager
- iStar Help Desk
- Click Commerce (if they are indicated in the plan)
- CHLA Data Center (where the servers are located)

## **5. Standard Operating Procedures Maintenance**

The integrity and validity of IRB proposal submissions, reviews, and approvals can be ensured by following the regulations and guidance of FDA, DHHS, and OHRP and the institutional policies regardless of changes in personnel. Written procedures must be in place to ensure the highest quality and integrity of the update and oversight processes of the iStar system and for the adequate documentation of such oversight.

### **5.1 Review, Revision, and Approval of SOPs**

- Changes to regulations, federal guidelines, system practice, or policies and procedures of USC and CHLA may require a revision to this SOP.
- SOPs will be reviewed by the iStar Site Manager at appropriate intervals.
- A track changes version of the SOP with all revisions marked shall be archived in an electronic format with the prior approved version of the SOP.

### **5.2 SOP Dissemination and Training**

- When SOPs are revised, they will be disseminated to the appropriate individuals and/or departments. A copy of the revised SOPs will be posted on the iStar system and /or IRB/OPRS websites for general dissemination to users.
- Training will be provided to all members of the iStar development team and IRB staff on any new or revised procedure.
- Each new iStar development team member employee must review all applicable sections of this SOP.

### **5.3 Responsibility**

- The iStar Site Manager is responsible for establishing and periodically reviewing and modifying (as appropriate) iStar standard operating policies and procedures.

### **5.4 Applicable Regulations and Guidelines**

- 21 CFR 11