

INFORMATION SYSTEMS

PROCEDURES MANUAL

September 15, 2012

Table of Contents

Table of Contents	2
MISSION STATEMENT	4
INTRODUCTION	4
HOW TO USE THIS MANUAL.....	4
ORGANIZATION	4
CONTACT LIST	5
Information Systems (IS).....	5
Systems Development Services (SDS).....	5
Systems Support Services (SSS).....	5
TDOC Help Desk.....	5
SYSTEMS SUPPORT SERVICES	6
HELP DESK	6
Network and System Security.....	6
Active Directory.....	6
Outlook Exchange.....	6
Single Sign-on.....	6
User Setup.....	6
User Revocation.....	7
User Access Change	7
Password Reset	8
Adding New Codes to TDOC Systems.....	8
LS/CMI – Level of Service/Case Management Inventory	8
Application Support (modify/deletion of data).....	9
Remedy	9
Network Support.....	9
Central Office Support Tracking	9
Global Messages	9
System Outage	9
Other, Non Outage Related.....	9
Site Coordinators	9
DESK TOP SUPPORT	10
P.C./Laptop Replacement	10
Imaging Standards	10
Process for Issuance of PC's/Laptop's	10
Process for Loaner Equipment.....	11
Service Request Process	11
Inventory Check List Process (Talk w/Sharon about transfer form)	11
TRAINING	12
Jail Training	12
TOMIS/eTOMIS.....	12
Distributed.....	12
DISASTER RECOVERY	12
PDCA's (PRODUCTION DATA CHANGE AUTHORIZATION).....	13
DOUBLE/MINGLED NUMBERS	13
SYSTEMS DEVELOPMENT SERVICES	15
PROJECT DEVELOPMENT	15
Project Management Office	15

Project Requests.....	15
Project Initiation.....	15
Feasibility Review	15
Project Phases	16
Project Tracking.....	17
User Requirements.....	17
Project Sponsors(s) and Subject Matter Experts.....	17
Project Teams and Assignments	17
DEVELOPMENT PROCESSES	18
Distributed.....	18
Mainframe.....	19
TESTING PROCESSES	21
Testing Team	21
Testing Preparation	21
User Acceptance	22
IMPLEMENTATION.....	22
Implementation Plan.....	22
Software Moves	22
Notifications (Help Desk).....	23
Training New Designs	23
SOFTWARE MAINTENANCE.....	23
Applications	23
Version Updates.....	24
REPORT DELIVERY	25
Crystal Enterprises (email)	25
INFOPAC/Document Direct.....	25
eTOMIS	25
Non-Recurring Reports/Extracts.....	25
COGNOS	25
Appendix.....	25
USER ID REQUEST FORM.....	26
LEVELS OF SERVICE / CASE MANAGEMENT INVENTORY (LS/CMI)	27
Production Data Change Authorization	28
PROJECT REQUEST.....	29
FEASIBILITY REVIEW	30
Test Plan.....	31

MISSION STATEMENT

Information Systems (IS) is tasked with providing management information, technical support and administrative services to all divisions of the Tennessee Department of Correction in the pursuit of their business goals and objectives.

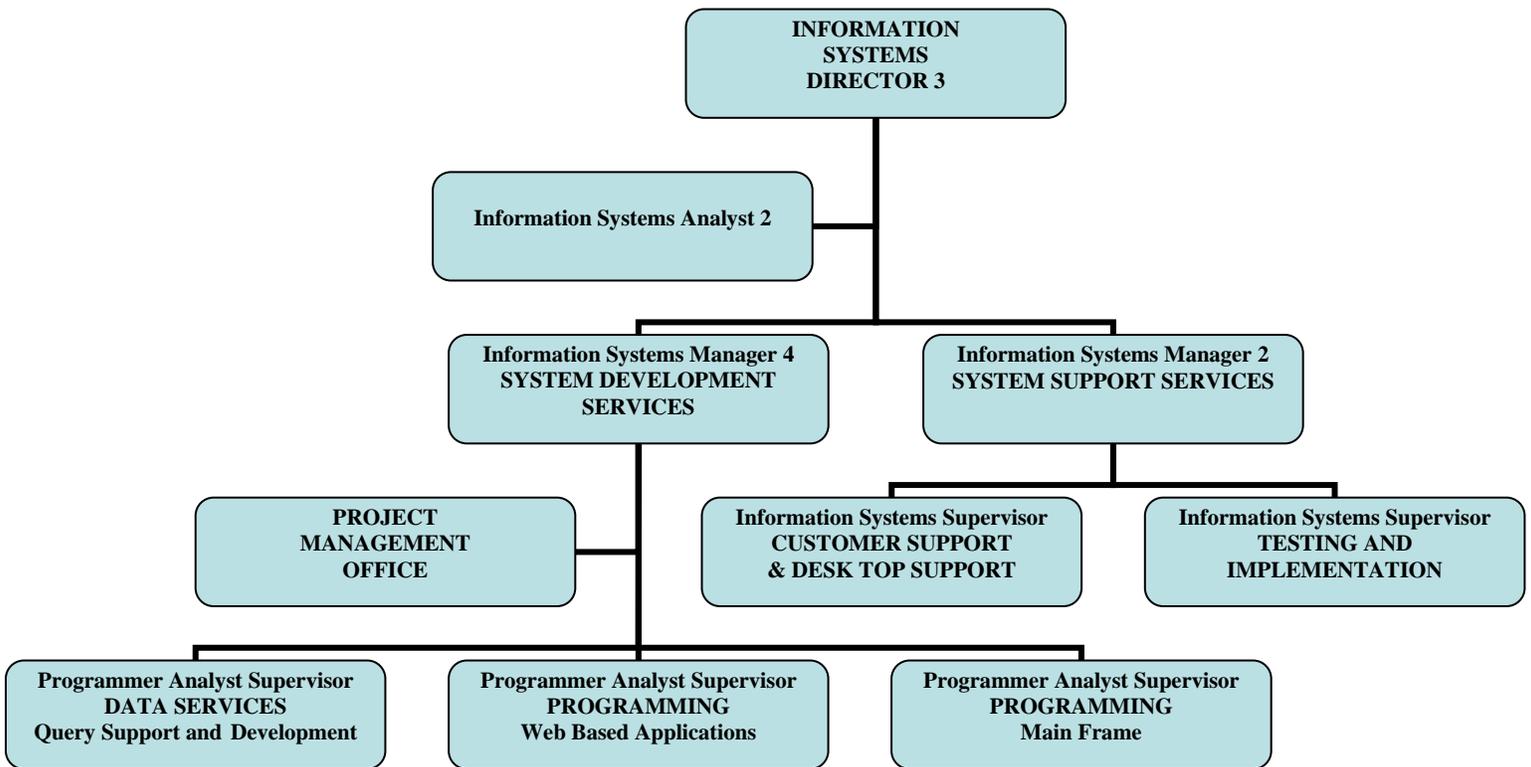
INTRODUCTION

Information Systems has developed this operational procedures manual to provide staff guidance and assistance, promote efficient and consistent operation and ensure procedural uniformity with enhanced cost effectiveness. Policy formulation and the operational procedures developed to implement these policies are a vital element in the development and application of good management information practices.

HOW TO USE THIS MANUAL

This manual provides an overview of the Information Systems division in the State of Tennessee, Department of Correction. The “Table of Contents” clearly defines the divisions, and their assigned tasks and responsibilities. Names and numbers are available in the “Contact List” section, for easy referral. Any questions or comments should be referred to the appropriate individual on the “Contact List” for each division. Updates will be supplied as necessary to keep this manual current.

ORGANIZATION



CONTACT LIST

Information Systems (IS)

Director: Don Baisden
Telephone: (615)741-1000 ext 8030
Email: Don.Baisden@tn.gov
Location: Fourth Floor, Rachel Jackson Building

Systems Development Services (SDS)

Manager: Kenneth Graves
Telephone: (615) 741-1000 ext 8091
Email: Kenneth.Graves@tn.gov
Location: Fourth Floor, Rachel Jackson Building

Systems Support Services (SSS)

Manager: Wayne Sisk
Telephone: (615) 741-1000 ext 8066
Email: Wayne.Sisk@tn.gov
Location: Fourth Floor, Rachel Jackson Building

TDOC Help Desk tdoc.helpdesk@tn.gov

Supervisor: Joel Conlin
Telephone: (615) 741-1000 ext 8065
Hepl Desk Cell: (615) 253-8222
Location: Fourth Floor, Rachel Jackson Building

SYSTEMS SUPPORT SERVICES

HELP DESK

Network and System Security

Active Directory

Is a state mandatory directory service created by Microsoft for Windows Networks. Active Directory provides a centralized platform for network administration and security. It authenticates and authorizes all users and computers in a Windows type network—assigning and enforcing security policies for all computers and installing or updating software.

The TDOC Help Desk submit RFS's (Request For Service) thru Remedy requesting Active Directory and Outlook Exchange accounts (Active Directory and Outlook Exchange passwords are synchronized) for central office staff only. In the request the Help Desk provides the User's name, ID, Phone #, and Job Title. Initially OIR will create the password with the account setup. Since OIR does not provide the Help Desk with the AD password it is changed by Help Desk staff that has Active Directory System Administration Accounts. The Help Desk staff then forward the changed password to the user. Users have access to change their AD password, however if the password is entered incorrectly the account is locked and the Help Desk must be contacted in order to have the account unlocked.

Outlook Exchange

Is a Microsoft email service adopted by the State of Tennessee in 2011 and used by TDOC. Although often used mainly as an email application, it also includes a calendar, task manager, contact manager, note taking, and journal.

The Help Desk requests the Outlook Exchange accounts at the same time the RFS is submitted for the Active Directory accounts. Outlook Exchange and Active Directory passwords are synched at the time the accounts are created so that users need only to remember one password. In addition to password resets the Help Desk also provide users with Outlook Exchange support.

Single Sign-on

Is a Tennessee Department of Correction application designed so that users can use a single password to access multiple web based distributed applications. The user's menu will only display applications to which that user has access. Although the RACF ID is used to identify the user the single sign-on password is not synched with the RACF password. The single sign-on application requires the password be changed every 90 days.

User Setup

All new users receive a User ID and password to access departmental systems. Central Office and non Department of Correction organizations are required to complete the User ID Request Form providing information such as home address, phone number, date of birth, SSN etc., in addition the Central Office user is given an Active Directory and Outlook Exchange accounts. For non departmental agencies such as the County Jails VPN (Virtual Private Network) and/or HOD (Host On Demand) accounts are set up. These accounts allow non departmental users to access the Department of Correction network/systems so that offender information can be updated.

New users for prison facilities are set up by the facility Site Coordinators who submit an email to the Help Desk requesting the User ID and password for new users; in addition they also indicate the applications the new user should have access to. Information Systems provide facility user setup of Active Directory and email (Outlook Exchange) accounts. [User ID Request Form](#)

User Revocation

All state and non state agencies wherein a system user/employee has access to the Department of Correction Information Systems and that user's employment is terminated, the employing agency should notify the Help Desk immediately following the termination so that all TDOC system access's can be terminated. The agency of termination is to submit an email to BI_Tomis_Staff_Removal indicating termination of the employee. Once the email is received the Help Desk staff will within one business day;

1. Revoke mainframe access via RACF and removes user ID from associated RACF groups.
2. Inactivate user access to all applications under Tennessee Department of Correction.
3. Submit a Request For Services (RFS) to have all state network access's, Including Active Directory, Outlook, VPN/HOD, etc., deactivated/removed for Central Office staff only. Field staff network deactivation is provided by Information Systems (IS).
4. Move the Staff Removal request to a secure folder and is to be kept for a period of 3 years.

A weekly Saturday morning batch process revokes a user's RACF ID 30 days after the user/employee last signed in.

Applications not dependent upon RACF security, distributed applications, the user is not able to sign in if the password has not been changed within 90 days, Help Desk assistance is required. The status does not change to inactive unless the Help Desk manually changes the status.

Should a situation dictate an emergency action to limit anyone's access to our systems, an authorized person may place a call to the help desk phone or cell phone 24 hours a day and request an Administrative Hold be put on the individual's ID. This action is merely a change of passwords so the individual may not log on with his active directory account pending further action. After the action has been approved, the standard processes take effect. Authorized to make such a request should be management level.

User Access Change

User system access is evaluated and assigned by the Help Desk based on email requests from central office management and Warden Designated Site Coordinators. The process for deactivating and reassigning accounts is relevant to consolidated/non-consolidated locations. A consolidated site is where the network servers are controlled by OIR "Office of Information Resources" versus non-consolidated sites, the site networks are controlled by The Tennessee Department of Correction.

1. Employee Transfer

- A. Facility to Facility – The user-id of the old site is revoked and inactivated on all TDOC applications (see User Revocation section) and a new user-id and access levels are created (see User Setup section). The Help Desk will send an email to the old and new site coordinators and BI_Tomis_Staff_Removal so that all interested parties are notified of the revocation and creation of user-ids. The old and new site coordinators are responsible for contacting ITS regarding removal/creation of Active Directory, FileNet, and Outlook accounts.
- B. Facility to Central Office – The Help Desk is responsible for revocation of old user-id and creation of new user-id. The Help Desk is responsible for creation of Active Directory, FileNet, and Outlook accounts and will contact ITS concerning any transfer of users retained electronic data. ITS assists in the copying of user transferred data to disk and also assist with the transfer of information from non-consolidated to consolidated active directory containers.
- C. Central Office to Facility - The Help Desk is responsible for revocation and creation of old and new user-id's, ITS is responsible for creation of Active Directory, FileNet, and Outlook accounts. The Help Desk assists in the copying of user transferred data to disk and also assist with the transfer of information from consolidated to non-consolidated active directory containers.

2. **Employee Job Change within the same location** -Job assignment changes may require access level changes within TDOC applications. When changes are requested by site coordinators/Central Office

Directors the Help Desk will make the appropriate changes to the individual's user group assignment.

3. Customized User Access Change - A user's current user group is kept and the user's access is customized according to the new job responsibilities associated with the user access change request.
4. Group Level Access Changes – All requests for adding/removing/modifying user groups require IT Director and Commissioner level approval.

Password Reset

Password resets require an email request to the Help Desk. Applications include, single sign on, RACF, TOMIS/eTOMIS, Active Directory (Outlook, FileNet/Capture Plus) LS/CMI, etc. Requests to the Help Desk are received statewide however Information Systems (IS) have the capability of resetting Active Directory related passwords for the institutions. The Warden Designated Site Coordinators have the capability to reset RACF passwords for their facility and staff from that facility should send their password reset requests to the Designated Site Coordinator.

Adding New Codes to TDOC Systems

TOMIS/eTOMIS

Request for new codes should be directed to the Director of IT. The Director of IT forwards the request to the Help Desk manager who reviews the request then forwards the request to the Legacy System Programmer Supervisor. Assigned analysts will review the request checking for programming logic that may or may not be linked to the codes table.

If a request involves Incidents/Infractions/Disciplinary, policy must be addressed.

1. Programming Logic not built into the codes table.

If the codes table has no programming logic associated with the codes table then with the approval of the sponsor requesting the code the Help Desk may proceed in modifying the code. To keep the codes in TOMIS/eTOMIS in synch the codes should be modified thru the eTOMIS application.

2. Programming Logic is built into the codes table.

If the codes table has programming logic associated with the codes table then this request must be established as a project and forwarded to the Project Management Group so that it may be entered into the project tracking database creating a project ID. Based on the difficulty of the request the project may require a review by the Management Advisory Committee (MAC).

Distributed Apps

Requests for new codes should be directed to the Director of IT. Once approved the request is forwarded to the Distributed Programming Supervisor who will have the requested codes added/modified.

LS/CMI – Level of Service/Case Management Inventory

MHS, Multi Health Systems, is a Canadian based application adopted by the Department of Correction Rehabilitative Services division as an assessment tool to measure the risk and need factors of late adolescent and adult offenders.

The Help Desk is responsible for user setup, access, password resets, and revocations of departmental users. Form CR3736 is required for user setup/access. [LS/CMI Form](#)

Application Support (modify/deletion of data)

Often users will make incorrect entries (often involving an incorrect offender ID entry) which require Help Desk staff assistance in modification or deletion of erroneous records. The vast majority of users do not have the ability to modify or delete entries within TDOC systems however users that have modify/delete capabilities have been authorized by high level management.

When a modification or deletion is needed users are to email their requests to tdoc.Helpdesk@tn.gov.

Deletions are handled by Help Desk staff who have been authorized by the Director of IT.

Modifications are normally handled in two ways.

1. Less critical data such as movements, cell bed assignments, staff assignments, etc. help desk staff often modify allowing the record to indicate the helpdesk staff id.
2. The more critical records such as classification, incidents, disciplinary, health/mental health, etc. require a PDCA (Production Data Change Authorization) in order that record user identifications are maintained. These records often have associated paper copies requiring offender signatures and thus require the original entry of staff ids and system ids be retained.

Remedy

Network Support

The Remedy System provides a consolidated Service Process Management platform for automating and managing Service Management Business processes. All requests for OIR related service (RFS) are submitted thru Remedy. Requests range from new user setup/access changes to user revocations.

Central Office Support Tracking

All Central Office users must submit service requests thru Remedy for desk top assistance and TDOC application support. Help Desk/Desk Top support staff will process the request and enter the actions taken into the Remedy system.

Global Messages

There are two types of Global Message and they are sent out by Outlook Exchange email and TOMIS email (LSWA).

System Outage

When system outages occur or planned the Help Desk Supervisor notifies all system users, TDOC, Jails, CCA, etc. of the outage and will specify systems and screens affected, date and time of outage if planned, and expected downtime if known.

Other, Non Outage Related

Non outage related message require Commissioner/IT Director level approval. These messages target specific users and are sent accordingly.

Site Coordinators

Institutional employees designated by Wardens recognized by the help desk as the Wardens Liaison concerning system issues. Requests are submitted for new user set up, user access changes, and user revocations. A Site Coordinator has password reset abilities, user status reset, reset user questions for TOMIS only; they do not have access to change or modify nor assign users to user class groups.

DESK TOP SUPPORT

P.C./Laptop Replacement

Replacements of Laptops are set at every 3 years, for PC's its every 4 years and the replacement schedule is heavily dependent upon funds available at the time of the needed replacement. Replacement priority should be given to the older equipment.

When replacing a pc/laptop, the user's files are either copied to their F Drive or to a flash drive or CD. Any specialty software is also noted that will need to be reinstalled on new pc/laptop. The pc/laptop is then reformatted and the operating system (Windows XP or Windows 7) is reinstalled. Basic software is reinstalled on the pc/laptop if there is no current image for that model pc/laptop.

If the pc/laptop is going to another person within the same section, then the pc/laptop can be left as is, with the exception of personal files belonging to the previous user, those files are deleted. A transfer form is completed for any equipment, pc/laptop/printer/scanner exchanges (in or out) taking place within The Department of Correction Central Office. This form is also used when equipment is surplused.

When a pc/laptop is replaced that has a bad hard drive, the KillDisk is ran on the pc/laptop if the pc/laptop can read the CD/floppy disk. Or the hard drive is removed and destroyed via a hole drilled into it or taken apart. For a pc/laptop that is being surplused (sent to TSP), the KillDisk software is applied to the hard drive erasing any previously stored software or data.

Imaging Standards

Policy 109.08, Expire July 15th 2012

FORMATTING STANDARDS FOR THE REISSUANCE OF TDOC PERSONAL COMPUTERS.

All pc/laptops are set-up with the basic software/applications.

When imaging a new pc/laptop, turned on for the first time, the updates for Windows are installed.

Other options (ex: power save options; firewall turned off, etc) are set for the pc/laptop. We then install Office 2003/2010; TN3270; Adobe Reader; SRAVPN software; office converter files; and Visio viewer.

The eTOMIS; Policy; and TDOC Intranet icons are added to the desktop folder. These icons will be placed on the user's desktop under their profile for that machine. Once complete an image is created.

Any specialty software (Adobe Acrobat; Visio; FileNet/Capture Plus; etc) is added to the pc/laptop when it is determined who is getting that pc/laptop.

Printers are added according to the location of the user. Example: a pc/laptop for an IT person would have the designated printers for the IT Division installed on that pc/laptop.

Process for Issuance of PC's/Laptop's

All requests for issuance of permanent PC's/Laptops must be approved by the TDOC IT Director. Upon receipt of the IT Director's approval, the issued PC/Laptop is imaged pursuant to the Imaging Standards. If the issuance is due to a replacement of unusable equipment, the old equipment is processed as per the imaging standards defined in the PC replacement section.

Process for Loaner Equipment

The loaner equipment is checked to verify updates are in place. The machine is profiled with the user information for workstation only. When the person picks up the equipment, that person must sign for it in the loaner log. When the equipment is returned, the IT person receiving it will date and initial the loaner log to indicate the return.

If the loaner equipment is leaving the building then the request must be in writing from the requesting persons Director.

Service Request Process

All Central Office and Probation and Parole users must submit service requests thru Remedy for password resets, desktop/laptop assistance, system support, staff removal/termination, new employee setup, etc. Help Desk staff will process the submitted request utilizing the Remedy work order functionality.

Users other than Central Office and Probation and Parole staff should submit email requests to tdoc.helpdesk@tn.gov for password resets, system support, new employee setup, etc. Staff removals/terminations, other than Central Office, staff will continue to submit requests to Bi_Tomis_Staff_Removal@tn.gov. These requests will be entered into the Remedy system by the Help Desk staff.

Inventory Check List Process

The Help Desk maintains 2 excel spreadsheets for inventory tracking of Central Office pc's, laptops, software, scanners and printers. These reports are updated each month.

Surplused equipment is removed from the report. Swapped or replaced equipment, the records are modified to indicate the change and with new equipment or staff a new record entry is made. Software licenses are returned to inventory.

Perpherials.xls - This file is used for tracking current inventory of printers and scanners and is updated by the BI-Tech Support group. Information listed is the Device Name, State Tag, Location and Comments. Since these devices have multiple users a User ID is not recorded.

UpdatedCOEquipment2012.xls - This file is used for tracking current inventory of PC's and Laptops assigned to Central Office staff and is updated by the Help Desk support group. Information listed is the User ID, Name, State Tag, Floor, Brand/Model, Comments, and a yes or no column for Office 2012.

Software Licenses – Are tracked by issued PC's. When PC's/Laptop's are surplused the software license is returned to inventory and updated on the list of available licenses.

TRAINING

Jail Training

eTOMIS training is provided by IT staff for county jail administrators and staff throughout the state as well as an occasional employee from The Department of Correction Central Office. Training is one day and conducted bi-monthly comprised of 10 to 15 attendees. Topics covered are system navigation, adding an offender, offender search, arrivals and departures, bonus credits classification, and how to enter program credits for offenders.

The class also includes short sessions with representatives of various Departmental Units such as Fiscal (Jail Board Bill), Classification, Sentencing, and Planning (Jail Report). These sessions usually last 15 to 30 minutes with a question and answer segment at the end of each session.

Training records are kept by IT listing attendees, the attendee's county jail, and dates of attendance.

TOMIS/eTOMIS

TOMIS/eTOMIS has a training environment. The TOMIS/eTOMIS Training Environment has a set of predefined training IDs. Each ID environment is independent from the other, so when one Training ID makes an update in the system, the change does not affect the other Training IDs environment.

The Training IDs range from BITC001 to BITC199. The training environment has a set of preexisting information. BITC001 to BITC100 is used by DCCO and the facilities. DCCO Jail Training uses BITC025 to BITC050. BITC101 to BITC150 is used by the Training Academy. BITC175 to BITC199 is used by BOPP.

Distributed

Distributed Training is conducted in the System Test Environment. Each person attending the training will have to be assigned to the Distributed Security, if not already, and the systems necessary for the training. Each ID is signed into the same system test environment, so when one User ID makes an update in the system, the change does effect the other User IDs environment.

DISASTER RECOVERY

Disaster Recovery refers to the procedures related to preparing for recovery or continuation of technology infrastructure critical to the Department of Correction after a natural or human-induced disaster. Once a year the Department of Correction participates in a mock disaster with OIR, Office of Information Resources, where lost data is identified, restored then verified correct by TDOC IT staff.

Disaster Recovery (DR) testing involves three dates. The first date is the actual date of the "assumed" disaster which comparative test data is gathered. The second date is the date of the imagined disaster or the "Target Date". The third date is the date of the actual DR test. For the target date the following actions are taken:

A series of queries are executed on selected TOMIS tables prior to the time of the assumed disaster and the resulted are saved.

- A series of INFOPAC reports that are prior to the assumed disaster date/time and representing as much data as possible are downloaded and saved
- Mainframe Programming Services will execute a process during the evening before the target date that counts the rows on each of the TOMIS tables and the results are saved.

On the DR Test date, the OIR DR Test group will restore the operating system from DR backup data to a remote mainframe system designated for the test. Next, the various systems are restored such as CICS, DB2 and others.

When we are informed that TOMIS has been restored the following steps are taken:

- The process that counts the rows of the TOMIS tables is executed.
- A slightly modified version the nightly batch process corresponding to the evening prior to the target date is run.
- The same queries that were run on the target date are submitted.
- Copies of the INFOPAC reports are printed.

Once these actions are complete, the results are compared to the results from the target date process. All discrepancies are analyzed. A summary report is created outlining the test results. If the discrepancy is minor it is reconciled. If it is major, it is noted in the summary report and added to the test script for future reference.

PDCA's (PRODUCTION DATA CHANGE AUTHORIZATION)

System users often make keying errors, need deleted data restored, miss data entry timelines or an expungment order is received requiring data to be modified/deleted. In order to correct these data issues IT staff must send an email with the PDCA email format, have it approved by the SSS Manager, and then the Manager forwards the email with approval to programming staff for data correction. PDCA email format below. [PDCA Form](#)

DOUBLE/MINGLED NUMBERS

With the introduction of TOMIS in February of 1992 a decision was made that offenders would be assigned one ID and that ID would be used to identify the offender. Due to inadequate searches/training users often assign additional numbers thus causing the existence of a double number.

The term "Double Number" is used to describe situations in which an offender has been assigned one or more TOMIS ID's. A "Mingled Number" is an instance of two or more distinct offenders with data mixed or "mingled" between them or in rare cases when two distinct individuals are entered on the same TOMIS ID.

These double numbers are reported either by a user or from a daily report that analyzes data from TOMIS ID's created the day before compared against existing TOMIS ID data. As the double/mingled numbers are reported they are entered into an Access database. The status of the double number issue is tracked from this database.

The procedure for processing double/mingled numbers has evolved from a 'trial and error' method into a more precise analysis of the data involved. Several tools are available to assist in the determination of whether the reported ID's are truly 'double' or 'mingled' numbers and are listed below, they are;

PDOUBLE: This is a QMF Procedure that creates a ‘map’ of the data associated with an offender ID.

CRIMINAL JUSTICE PORTAL: This is a distributed application administered by the Administrative Office of the Courts. This application includes TOMIS data, Drivers License information and TBI arrest information.

TID-SID Access database: This is an Access database created from data provided by TBI in 2005. It contains SID, FBI #, Name, DOB and SSN. Any name under which the offender has been arrested is included.

Once a determination has been made as to which offender ID is to be retained (usually the number with the most amounts of data is retained) the data is processed by one or more of the following methods:

Automatic Transfer: The conversation LSWL, TOMIS ID Maintenance, has the ability to automatically transfer data from a number of TOMIS conversations.

Manual Transfer: This involves entering data from the ID to be deleted on the ID to be retained then deleting that data from the ID to be deleted.

Production Data Change Authorization (PDCA): A request to Mainframe Programming Services to overwrite the TOMIS ID to be deleted with the TOMIS ID to be retained using a database manipulation tool. It is used for those bits of information that cannot be processed by any of the other methods.

Judgment Order Move/Deletion: Sentence Management Services (SMS) is tasked with entering a judgment order (JO) from the delete ID on the ID to be retained then deleting the judgment order from the delete ID once it is determined that the entered JO has calculated correctly. In some cases all that is needed is the deletion of the JO from the delete ID. Only SMS can perform these functions.

Facesheet Image Deletion: When an image exists for the TOMIS ID to be deleted an authorized user will log into the Facesheet Administration Application (there is a link on the TDOC Intranet home page). From this location the image(s) can be deleted.

When the double number issue has been resolved the person that reported the double number is notified. A Contact Note is entered on the retained ID using the contact code “DNBR” to record the occurrence of the double number.

SYSTEMS DEVELOPMENT SERVICES

PROJECT DEVELOPMENT

Project Management Office

The Project Management Office (PMO) purpose is to deliver project support to TDOC by providing guidance in project management processes and methodologies in a manner that is efficient, consistent, and standardized and to provide mentoring and coaching in an effort to raise the project management skill level of the division.

Project Requests

Project Initiation

All system and report update requests must be submitted to the Project Management Office (PMO) at BI-TDOC-Project-Mgmt@tn.gov using the [Information System Project Request Form \(CR-3782\)](#). The request must originate from a Commissioner, Director or Warden. The request shall include the requestor name, sponsor, type of request, brief description, areas affected, if policy is affected, prerequisites, requested completion date, and the reason for the requested completion date. If policy is affected by the project, the requestor is responsible for updating the policy.

The request is first reviewed by the PMO to ensure the form is complete or has enough information. At the time the request has enough information to proceed, the request is assigned a number.

A report request includes data requests and extracts. The report request will be sent to the appropriate staff. If a resource is available, a resource will be assigned to the report and sent to the appropriate staff to complete the request. If a resource is not available, the request is temporality put on a hold status. Either outcome will be communicated to the requestor.

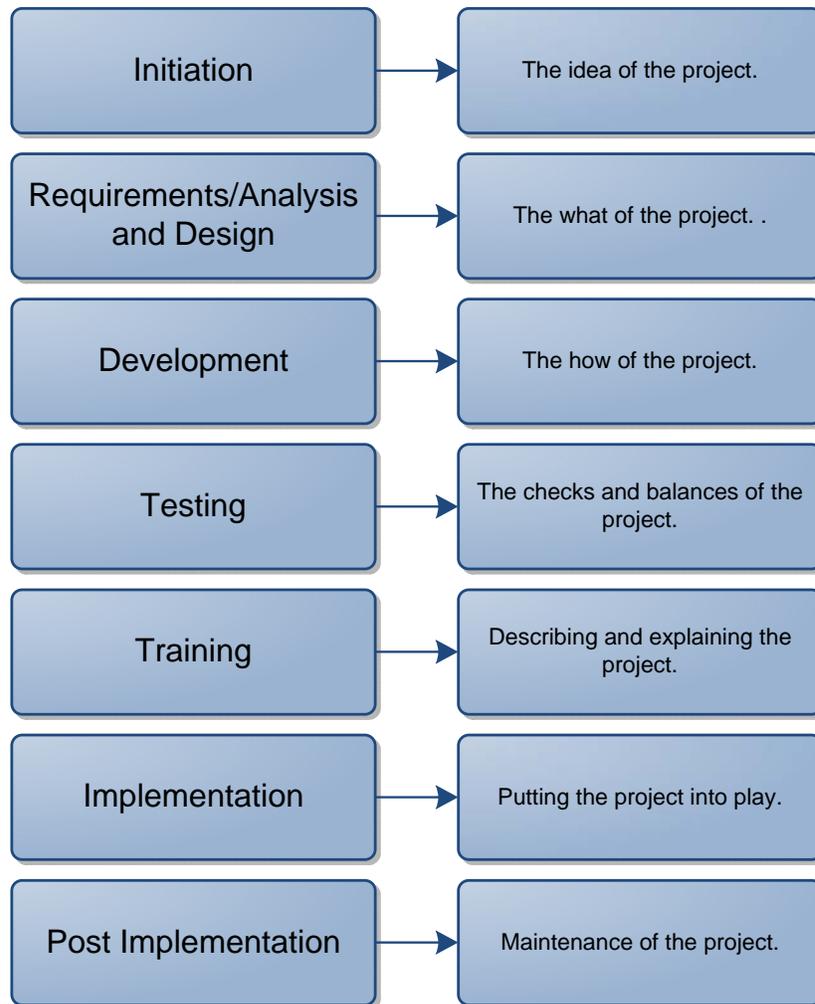
A system update request will be discussed between management and the PMO. If a resource is available, a resource will be assigned and sent to the appropriate staff requesting the completion of the Feasibility Review Form ([CR-3783](#)). If a resource is not available, the request is temporality put on a hold status. Either outcome will be communicated to the requestor.

Feasibility Review

A system update request may require a Feasibility Review, which consists of the assigned resource and requestor discussing and documenting the scope. The review also includes the request's estimated work hours, a description of the work, and required new hardware or software. *See Feasibility Review Form [CR-3783](#)*. Upon the completion of the Feasibility Review, management and the PMO discuss if further approvals are required. Upon approval of the continuation of the request a project number will be assigned. If resources are available, resources will be assigned to the project and sent to the appropriate staff to complete the request. If a resource is not available, the request is temporality put on a hold status. Either outcome will be communicated to the requestor.

Project Phases

The following is the most common order and phases of a project: Project Initiation, User Requirements/Analysis and Design, Development, Testing, Training, Implementation and Post Implementation. The exact phases and the order, in which the phases are completed, may vary slightly, depending on what needs to be achieved with the project. A project plan is usually created using the project phases as the main summary tasks.



Project Tracking

Projects status and information is kept in the Request Tracking System. Such information includes the project's request date, the sponsor, subject matter experts, resource assignments, project phase dates and areas for comments. The project entry is updated throughout the project phases.

User Requirements

User Requirements is a phase of the project life cycle. The requirements can include information gathering, meetings, surveys, interview, analysis and design. The initial Feasibility Review gathers high level user requirements. If the project is approved to continue with resources and the project needs more detailed requirements, a User Requirements Document (URD) is prepared. A URD is the details of what needs to be completed in order to fulfill the project request. The URD may need to go through several revisions before key stakeholders and IT Team Members approve the document. The sponsor and other key stakeholders must approve or sign-off on the URD prior to starting the System Development phase. The sign-off signifies the approval and agreement of the documented requirements and design. The URD is used for System Development and Test plans, if changes need to be made to the URD an **IT Project Change Form** should be completed and approved.

Project Sponsors(s) and Subject Matter Experts

A Project Sponsor represents the project at management level. The Project Sponsor must be a director, warden or commissioner level, although a designee or requestor can be appointed for working with the IT Team on the project. The Project Sponsor reads and signs-off on project documents. The Project Sponsor is the main communicator with stakeholders and users.

Subject Matter Expert (SME) is a person with special knowledge or skills in a particular area of the project. A project can have multiple SMEs. SMEs are heavily involved in the requirements/analysis and design, user acceptance testing and training phases of the project.

Project Teams and Assignments

Project Team Assignments are initially completed after the Feasibility Review is completed and the PMO and management have discussed available resources. A resource can be removed from the project or the work time allocated for the project can be updated. Resource updates are communicated to the necessary parties.

DEVELOPMENT PROCESSES

Distributed

The Distributed Application Development team is responsible for programming and testing ETOMIS and all web applications, crystal reports (scheduled and application), and the stand-alone Microsoft access application.

Review Project Requirements Document

When the Project Requirements Document is received, it is reviewed to determine if additional information is needed before the detailed program design is initiated.

Programming

- Database Creation:

Programmers on the Distributed Application Development Team create and maintain databases in the Test environment using the following:

Tools: TOAD (Oracle), SQL Server, Microsoft Access

When a database has been created, the programmer informs the supervisor, who is responsible for reviewing the database.

- Source Code:

Programmers on the Distributed Application Development Team create and maintain the program source code using the following:

Languages: C#, VB

Tools: Visual Studio (2005, 2008, 2010), Crystal Report XI, Visual Source Safe

The source code for is maintained in Visual Source Safe. This product allows for current and archived versions of the source code.

- ETOMIS Source Code:

Upon receiving notification that the BMS Map is created on the Mainframe, an import of the BMS Map is done in ROSCOEC. Format changes are done and exported. Once exported, the BMS map is downloaded using Attachmate and copied to Lotus 123. A macro is executed in Lotus 123 that will change the format to the required format for ACE (Software AG, formally Jacada). The context of the new text file is saved with a .bms extension. The .bms file and a screen capture from ACE is used to create the new ETOMIS screen. The programmer created the code in ACE software per user requirements. The source code is compiled to create a runtime.

- Unit Test:

Programmers, upon completion of the source code, test the application locally on their pc.

- Move Application to Development Web Server:

Programmers publish the web application to the development web server.

For ETOMIS, the runtime will be moved to the ETOMIS Test Server.

- System Test:
The supervisor is informed by the programmers when the web application is ready to be moved to the system test web server. The supervisor will have another programmer test the application in system test per user requirement document. Any issues found will be returned to the programmer. Once the programmer is satisfied with the application, the supervisor will notify the Project Management Team that the application is ready for System Testing. Any issues found in system testing and/or user testing will be return to programmer. Any changes made by the programmer will be moved to the system test environment for another round of testing.
- Production:
After receiving notification from the Project Management Team and the user has accepted the application, the database will be created in the Production Environment. For Oracle, a RFS is submitted to have the OIR Database group move the database from the Test Environment to the Production environment. For the SQL Server, the database is moved from the test environment to the production environment by the supervisor. The supervisor will move the published application on the Test Web Server to the Production Web Server. Once completed, the supervisor will notify the Project Management Team that the application is available in Production. Any scheduled crystal reports will need to be setup in the crystal server environment or schedule on the Production Web Server.
ETOMIS runtime will be moved to both ETOMIS Production Servers (2 Servers for Volume and Load Balance). The ETOMIS training runtime will be moved to the ETOMIS Training Server.
- Visual Source Safe Update:
The supervisor will move the source code from the visual studio test area to the production area. The source code from the test area will be removed. For ETOMIS source, a jpack will be created, which is also saved in source safe.
- Documentation Update:
The programmer will be responsible for updating the Distributed Application Inventory Document with any new application.

Mainframe

The Mainframe Application Development team is responsible for programming and testing TOMIS applications.

Review Project Requirements Document

When the Project Requirements Document is received, it is reviewed to determine if additional information is needed before the detailed program design is initiated.

Detailed Program Design

When a programmer assigned to a project has determined the Project Requirements Document is complete, detailed program design is initiated. During this phase, the programmer creates the following entities using the Design/1 software:

Detailed Program Specifications (SPEC) and Cover Pages (COVER)

Elements (D710)*

Screens (D320) and Screen Groups (D321)*

Copybooks (D615)

Database Designs (D073)

Codes Tables (D730)*

* indicates this entity is uploaded to the mainframe Install/1 repository.

Upload Entities to Install/1 Repository

Once they are created, those entities listed above with an asterisk are uploaded to the Install/1 online repository in CICS. These will be generated as CICS load modules using options found in the repository software.

Programming

- **Source Code:**

Programmers on the Mainframe Application Development Team create and maintain program source code using the following:

Languages: COBOL, CICS, DB2

Tools: Design/1, Install/1, TSO, CA-Librarian, Reflection 3270

The source code for programs and copybooks is maintained using ELIPS (Extended Librarian Interactive Productivity Services) in CA-Librarian. This product, along with CCF (Change Control Facility) enables the programming staff to maintain current and archived versions of the source code.

- **Load Modules (Executables):**

New and/or modified programs are compiled and linked as executable modules using the Install/1 Source Management Facility in TSO. Depending on the type of program compiled, the load modules are linked to the appropriate test load library for unit testing by the programmer.

Unit Testing

When a new/modified executable module is linked into the appropriate test CICS or batch region, the programmer is responsible for testing the module to ensure it performs according to the detailed program specification created during the detailed design phase. If programming problems are encountered, the programmer is responsible for making necessary modifications to the source code and re-creating the executable module for re-testing. If a design issue is encountered, it is the responsibility of the programmer to notify the project facilitator so the issue can be escalated to the appropriate decision maker, (up to the Project Sponsor), so the detailed design document can be modified to reflect the corrected design. Once the programming team receives the corrected design document, the change(s) will be made to the appropriate detailed design entities and the program source code. Once recompiled and linked, the program(s) will be re-tested to ensure correct functionality according to the newly updated design document.

Program (Executable Module) Migration

Executable modules are migrated to other regions using the OIR-supported TSO utility "PRODMOVE." Modules are first migrated from the Unit Test region to the System Test region (see System Testing). Once all testing is done in the System Test environment and the project sponsor has completed all acceptance testing of the affected modules, PRODMOVE is used to migrate the modules from the System Test environment to Training and Production environments.

System Testing (Programmer)

The programmer is responsible for testing all affected executable modules in the appropriate system test CICS or batch environment to ensure that all affected entities were properly migrated to the system test environment. Once this testing is completed, the programmer will notify the project facilitator that the programmer system testing is completed and is now ready for acceptance testing by the testing team and the project sponsor.

TESTING PROCESSES

Testing Team

The System Test Team consists of one to three individuals from the System Support Services group. Prior to the execution of an actual Test Plan, several steps need to take place.

Testing Preparation

Review the Project Requirements

The Test Team will get an overall feel for what the project is to accomplish. One team member may be excluded from the review and be allowed to test blindly using only the knowledge of the functionality of other TOMIS/eTOMIS conversations or Distributed applications.

Determine Application Environment

Is the application mainframe or distributed?

Analyze Data Requirements

Review the existing System test data to see if it will allow for a complete and thorough Test. If adequate data is not present, search the Production environment for data to satisfy the test requirements and have the programming staff move that data to the test environment. If data conversion was not performed and there are new data tables/fields, data will have to be created from within the application.

Create a Test Plan Document with Test Cases

Develop the test plan by which the Test Team will conduct System Testing. Each test case will be designed to expose possible flaws in the application logic, insure that all edits perform as expected, make sure that Navigation is intuitive and that application security allows only authorized users to access the conversation or application. [Test Plan](#)

Application Areas for Testing

1. Security/Access-When testing the conversation/application security it is important to determine that only authorized users are able to access the application. User Classes are used to define the level of access in TOMIS/eTOMIS. Additional security tables may be used to further restrict access to certain portions of the application. These also need to be tested. An example is table **TDHS370 - MNTL HLTH STFF ACCESS TBL** which restricts full access to only Staff ID's contained in the table.
2. Navigation – Navigation testing will include insuring that any function keys operate as they should and links to other areas operate as described in the project packet.
3. Functionality – The application will be designed to accomplish one or more functions. These functions may be nothing more than data entry or they may be designed to perform a specific calculation, either on numeric data or on dates. The Test Plan should test both the expected and the unexpected. If there are data restrictions it must be determined that any error messages are working properly. Do data edits function as intended?
4. Appearance - Check the appearance of each application page. Is it readable? Are labels spelled correctly? Are any data fields 'truncated'? Is the look and feel consistent throughout the application?

Create an Issues Tracking Document with Open & Closed Issue Tabs

An Excel spreadsheet is used to record "Open Issues" any issues that may arise during testing and "Closed Issues" once they have been resolved.

User Acceptance

User Acceptance testing is very similar to System Testing. The big difference is that Test Cases should be developed by the user based upon his or her knowledge of the Business Function. For example, Sentencing would test a new sentence calculation based upon their specific knowledge of how other similar calculations work. In some instances, the System Test Team may have to assist the users in developing their test cases.

At the end of the testing phase a few short paragraphs are written describing the test, any issues that arose and their resolution. These may assist in preventing further occurrences of that type of issue.

IMPLEMENTATION

Implementation Plan

Implementation is the process of moving programs from the System Test environment, after testing is complete, to the Production environment. As a general rule, Implementation dates are the 1st and the 3rd Thursday of each month unless otherwise authorized by the IT Director. The Helpdesk will be contacted in order to notify users of the coming implementation and possible interruptions in service.

The Implementation plan will list all participants, their roles and responsibilities and the dates of completion. There will also be a section in which any issues or comments can be recorded.

Upon Implementation completion, the project analyst will enter the application and scan key areas for potential problems. The TDOC Helpdesk will send out another notification once the implementation is complete. This notification should include instructions to notify the TDOC Helpdesk if any issues are found and that person will be instructed to forward the issues to the project analyst.

Post-Implementation will involve one or more System Test and Implementation Team members logging into the application and check for obvious problems in navigation and appearance. After a pre-determined period of time (1-2 weeks) if no problems are found or reported, the project can be closed.

If issues are found, the project facilitator will have the requirements revised and send them to the programming staff for changes. After the changes are complete, the application will be System Tested once more with a revised Test Plan and Implementation Plan.

Once the project is closed, a System Test and Implementation Team member will write a few paragraphs describing the System Test as well as the Implementation process and note any issues found and their resolution(s). This summary will be placed in a folder called System Test and Implementation Summary within the project miscellaneous folder.

Software Moves

Software moves are discussed under sections Development Processes Distributed and Mainframe. Software moves are also mentioned in section Version Updates and Implementation Plan. We may want to consider removing this section.

The Department of Correction is a 24/7 operation comprised of more than 5,000 employees. It is important that employees be aware of software moves so that interruptions of employee schedules take up the least amount of time. A good example would be the Tennessee Correction Academy. Computer classes can be scheduled accordingly by being aware of routine dates and times of system changes due to software moves. Software moves are routinely scheduled for the 1st and 3rd Thursday of each month. Occasionally an emergency move is necessary and these require prior approval from the IT Director.

All software moves, scheduled or unscheduled will be preceded by an announcement, usually two announcements, 3 to 4 days prior to and the day of the move, informing all users of the date and time of the move, what systems are affected, how they are affected and the expected downtime. Some software moves require no downtime and therefore can be moved at anytime. If there is no downtime, no change in design/look or no change in functionality an announcement is not required.

Notifications (Help Desk)

Notices to users of TDOC applications are sent whenever system outages are planned due to OIR system maintenance or TDOC IT needs for installation of application changes. It is the goal to send these notifications not later than a week ahead of the scheduled outage so that users can make plans for the outage period or in the case of TDOC IT planned outages, the users can express concerns with the outage schedule that may require an alteration to the plan.

Additional notification should be sent the day of or the day prior to the outage as a reminder to the user community.

Follow up e-mails may or may not be sent notifying users of the availability of the applications upon completion of the outage processes.

All TDOC global e-mails will be sent via the State e-mail system and via the TOMIS e-mail system for those not having access to the state e-mail system.

Training New Designs

At times training is requested upon the completion of a project that consists of a new design or large modification to a system. With assistance from the project sponsor, a user manual is created. The project sponsor arranges the trainees, the location and necessary equipment. Other items are necessary to setup for training, see the Training section.

SOFTWARE MAINTENANCE

Applications

Software maintenance is the process of modifying a software system or component after delivery to correct faults, improve performances or other attributes, or adapt to a changed environment.

This definition reflects the common view that software maintenance is a post-delivery activity: it starts when a system is released to the customer or user and encompasses all activities that keep the system operational and meet the user's needs.

Corrective maintenance: reactive modification of a software product performed after delivery to correct discovered faults.

Adaptive maintenance: modification of a software product performed after delivery to keep a computer program usable in a changed or changing environment.

Perfective maintenance: modification of a software product performed after delivery to improve performance or maintainability.

Emergency maintenance: unscheduled corrective maintenance performed to keep a system operational.

Version Updates

From time to time there are software release updates. If the release is designated as a security update, you should apply the update as soon as you can with the authorization of the IT Director. Otherwise, you will apply the update according to implementation standards which are the 1st and 3rd Thursday of each month. There are also major release upgrades.

Before the update is applied it is important to know the difference between major and minor version releases. In most cases a major update is identified by the change of the number before the first decimal. For example if the current version is 6.5 and the new update is 7.0 this would often be considered a major upgrade to the current application. Major releases may include new tools, structure changes, changes to appearance and functionality. Minor releases such as 6.5 to 6.6 would include security issues or newly discovered bugs, flaws or errors in the source code of the application that produce an incorrect or unexpected results.

Considerations to take into account when upgrading from one release to the next.

1. See the instructions in the txt file of the download or handbook if available.
2. Upload the new version to a development/test site for testing.
3. Make sure that all the contrib modules have an upgrade path or possibly upgrade them individually.
4. Read and follow any instructions regarding upgrading any permissions modules that are being used. Many have specific steps we need to take before starting the upgrade.

Checking to ensure the upgrade process was successful.

1. Test each content type by adding new content.
2. Determine if any existing content has been corrupted or altered.
3. Ensure all modules and sub-modules required are enabled and active.
4. Ensure navigation and menus are working correctly.
5. Double check if any modules have introduced or changed permissions.

These processes may change depending on the type of software and version being updated.

REPORT DELIVERY

Crystal Enterprises (email)

Reports can be defined and stored on the Crystal Enterprise server and sent to an individual or distribution list by email on specific dates or intervals (daily, weekly, etc.) These reports are generally delivered as PDF documents or spreadsheets, and can gather data from multiple sources.

INFOPAC/Document Direct

INFOPAC reports are retrieved through the Document Direct application and can be scheduled to run on specific dates or intervals. Current reports, as well as a limited number of historic reports, are available for download. Real- Individuals requiring reports or extracts for one-time or non-recurring use can request these through the Director or his/her designee(s). Timeframes and formats may be subject to constraints imposed by other pending projects or requests.

time reporting is not available through Infopac, and all data must come from the mainframe (TOMIS) tables.

eTOMIS

Crystal Reports can be set up to be accessed through eTOMIS or other TDOC web applications and these reports are available on demand in PDF or Excel formats. They can be set up to retrieve batch data or real-time data, and can gather data from multiple sources.

Non-Recurring Reports/Extracts

Individuals requiring reports or extracts for one-time or non-recurring use can request these through the Director or his/her designee(s). Timeframes and formats may be subject to constraints imposed by other pending projects or requests.

COGNOS

The Tennessee Department of Correction will implement the COGNOS reporting tool in FY2013 which will provide dash boarding and other yet-to-be-determined data reporting capabilities..

Appendix



TENNESSEE DEPARTMENT OF CORRECTION

USER ID REQUEST FORM

HelpDesk: (615) 253-8222 Fax: (615) 741-6579

PART I. REQUESTING OFFICIAL

DATE:

REQUESTED BY:

AGENCY:

WORK SITE:

TELEPHONE #:

TITLE:

PART II. USER / EMPLOYEE INFORMATION

Last Name:

First Name:

Home Address:

City:

State:

Zip:

Home Phone:

Check here if this is a non-published number

Work Phone:

Fax:

Race:

Sex:

DOB:

SSN:

 Last 4 digits only:

Title:

Email:

Work Site:

Internet connection:

Local Network

Cable/DSL

Dial-up

Other:

DO NOT WRITE BELOW THIS LINE / FOR OFFICIAL USE ONLY

Assigned User ID:

Assigned Staff ID:



TENNESSEE DEPARTMENT OF CORRECTION
**LEVELS OF SERVICE / CASE MANAGEMENT INVENTORY (LS/CMI)
ACCESS REQUEST**

PART I. SUPERVISOR INFORMATION

Supervisor Name: _____ ID _____
Agency: _____ Work Site: _____
Work Phone: _____
Email Address: _____

PART II. USER INFORMATION

Requested For: _____ ID _____
Agency: _____ Work Site _____
Work Phone: _____
Email Address: _____

PART III. ACCESS LEVEL REQUESTED

SECURITY ADMIN: _____ **USER ADMIN** _____
OFFENDER ADMIN: _____ **VIEW ONLY** _____

PART IV. TRAINING CERTIFICATION/AUTHORIZATION (not required for view only requests)

Date Completed: _____
TRAINING LEVEL: **FULL LS/CMI** _____ **DATA ENTRY ONLY** _____
Certified/Authorized by: _____ ID _____
Work Site: _____ Work Phone _____
Email Address: _____

PART V. SUBMITTED BY INFORMATION

Date Submitted: _____

Submitted by: _____ ID _____
Work Site: _____ Work Phone _____

PART VI. *For Help Desk Usage Only*

Training Access Inactivated _____

Request Number: **XXXX**

Priority:

Medium

**TDOC Information Systems Division
Production Data Change Authorization**

Assigned Analyst:

Telephone/Ext.:

Requestor/User:

Date Requested:

Location:

Reason for Change:

Application:

Selection Criteria:

Data Items to Change:

Change Value From:

Change Value To:

Authorized By:

Date Authorized:

Use only if needed:

Addendum Criteria:

Addendum Date:

TO BE COMPLETED BY
Mainframe Programming Services

Table Affected:

Elements Affected:

Changed By:

Changed Date:

Notification Date:



TENNESSEE DEPARTMENT OF CORRECTION
 INFORMATION SYSTEMS (IS)
PROJECT REQUEST

All information sections on this form are required.

Requestor Name		Sponsor	
<i>Name of person responsible for the request</i>		<i>Name of the sponsor (director level or higher)</i>	

Division of Requestor	
------------------------------	--

Type of Request (<i>mark all that apply</i>)	
<input type="checkbox"/> New System	<input type="checkbox"/> Update to Existing System
<input type="checkbox"/> Data Request/Report/Extract – One Time	<input type="checkbox"/> Data Request/Report/Extract – Multiple Times
<input type="checkbox"/> Update to Data Request/Report/Extract	<input type="checkbox"/> Other (<i>please describe</i>) Click here to enter text.

Briefly Describe Request
<i>Click here to briefly describe the project request. Include the project needs, goals, benefits and objectives.</i>

Areas Affected
<ul style="list-style-type: none"> Click here to list division areas and/or processes

Policy	
Is policy affected? (<i>Please confirm with sponsor</i>)	Y/N Choose an item.

Prerequisites
<i>Are there any other tasks or projects that must occur prior to this request.</i>

Requested Completion Date	
Requested Completion Date or Schedule	Click here to enter a date.
Completion Date Reason (<i>mark all that apply</i>)	
<input type="checkbox"/> Legislation	<input type="checkbox"/> A prerequisite for another project
<input type="checkbox"/> Contract/Grant	<input type="checkbox"/> Other (<i>please describe</i>) Click here to enter text.

Save the completed form and e-mail the form as an attachment to IT Project Management by holding Ctrl and [clicking here](#)



TENNESSEE DEPARTMENT OF CORRECTION
 INFORMATION SYSTEMS (IS)
FEASIBILITY REVIEW

Requestor Name	
<i>Name of person responsible for the request</i>	

Reviewer	
<i>Name of the sponsor (director level or higher)</i>	

High – Level Scope
<i>What is in and out of scope for this project request? The scope identifies and describes the actual functions, features and deliverables of the project. This statement sets the tone and boundaries for the remainder of the project and is essential in all areas of a project life cycle from initiation to implementation. If the project is guided away from the scope, a change request form with new estimates will have to be created.</i>

Work Estimates										
<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%; padding-right: 10px;">Analysis:</td> <td>Enter the # of estimated Work Hours.</td> </tr> <tr> <td style="padding-right: 10px;">Coding:</td> <td>Enter the # of estimated Work Hours.</td> </tr> <tr> <td style="padding-right: 10px;">Testing:</td> <td>Enter the # of estimated Work Hours.</td> </tr> <tr> <td style="padding-right: 10px;">Implementation:</td> <td>Enter the # of estimated Work Hours.</td> </tr> <tr> <td style="padding-right: 10px;">Total:</td> <td>0 (To update total, right click and select update field)</td> </tr> </table>	Analysis:	Enter the # of estimated Work Hours.	Coding:	Enter the # of estimated Work Hours.	Testing:	Enter the # of estimated Work Hours.	Implementation:	Enter the # of estimated Work Hours.	Total:	0 (To update total, right click and select update field)
Analysis:	Enter the # of estimated Work Hours.									
Coding:	Enter the # of estimated Work Hours.									
Testing:	Enter the # of estimated Work Hours.									
Implementation:	Enter the # of estimated Work Hours.									
Total:	0 (To update total, right click and select update field)									

Work Description
<i>The hours estimated are based on the work needed to complete the project. (i.e., a new screen, tables)</i>

Hardware/Software	
Is there any new hardware or software?	Y/N <input type="text" value="Choose an item."/>
<i>If yes, please explain.</i>	

Test Plan

Test Cases	Test Area: <i>Security, Navigation, Functionality, Appearance</i>	Expected Results	Status: Pass - Fail	Observed Results / Comments
Test Case 1 <Enter Case Description - Include TOMIS ID when applicable>				
Scenario 1 <Enter Scenario Description>				
Scenario 2 <Enter Scenario Description>				
Test Case 2 <Enter Case Description - Include TOMIS ID when applicable>				
Scenario 1 <Enter Scenario Description>				
Scenario 2 <Enter Scenario Description>				
Test Case 3 <Enter Case Description - Include TOMIS ID when applicable>				
Scenario 1 <Enter Scenario Description>				
Scenario 2 <Enter Scenario Description>				