# ATTACHMENT 1
# STATEMENT OF WORK

# ATTACHMENT 1

# STATEMENT OF WORK

## 1. PURPOSE

The purpose of this Statement of Work (SOW) is to define the tasks and responsibilities of the Prime Contractor and the State during the term of this Contract.

## 2. SERVICE AVAILABILITY

The services shall be provided 24-hours a day, seven (7) days a week. This requirement for service availability may only be constrained, on an individual location basis, where 24-hour access is restricted, and where this access restriction is beyond the control of the Prime Contractor.

## 3. PERIOD OF PERFORMANCE CONTRACT TERM

The Contract Term shall be six (6) years with four (4) one-year optional extension years. The Prime Contractor shall not commence working until Contract execution.

## 4. ADMINISTRATION OF CONTRACT

The California Department of Technology (CDT) will administer this Contract on behalf of the California Department of Corrections and Rehabilitation (CDCR). The Prime Contractor will work with the CDT point of contact for issues such as Contract amendments. The CDT will be the Contracts Manager.

| State Department:<br>California Department of Technology | Prime Contractor:<br>Global Tel*Link Corporation |
|---|---|
| Division/Unit:<br>Statewide Telecommunications Network Division, (STND) Contracts Management Section | Unit/Department<br>Director – Field Service |
| Attention: Gerard Negrete | Attention: Michael K. Patterson |
| Address: P.O. Box 1810<br>Rancho Cordova, CA 95741-1810 | Address: 819 Striker Avenue,<br>Suite 16, Sacramento, CA 95834 |
| Phone: (916) 657-9190 | Phone: (916) 774-0533 |
| Fax: | Fax: (916) 921-1608 |
| Email:<br>CIOSTNDCDCRContractAdminUnit@state.ca.gov | Email: michael.patterson@gtl.net |

The CDCR will provide a CDCR Operations Manager. The CDCR Operations Manager is the point of contact for the day-to-day activities, Transition-In and Transition-Out of services, moves, adds, and changes, coordination of gate clearances, as shown in SOW, Exhibit A, Gate Clearance Informational and Approval Sheet; SOW, Exhibit C, Primary Laws, Rules, and Regulations Regarding Conduct and Association with State Prison Inmates and all other responsibilities as described throughout this Contract.

| | |
|---|---|
| State Agency:<br>California Department of Corrections and Rehabilitation (CDCR) | Prime Contractor:<br>Global Tel*Link Corporation |
| Division/Unit:<br>Enterprise Information Services<br>Infrastructure Services | Unit/Department<br>Director – Field Service |
| Address:<br>1960 Birkmont Drive<br>Rancho Cordova, CA 95742 | Address: 819 Striker Avenue,<br>Suite 16, Sacramento, CA 95834 |
| Attention: Kelley Graham IWTS/MAS Operations Manager | Attention: Michael K. Patterson |
| Phone: (916) 358-2640 | Phone: (916) 774-0533 |
| Fax: (916) 358-2619 | Fax: (916) 921-1608 |
| Email: Kelley.Graham@cdcr.ca.gov | Email: michael.patterson@gtl.net |

## 5. NOTICES

All Notices required by or relating to this Contract shall be in writing and shall be sent to the State contact representatives described in SOW Section 4, Administration of Contract.

## 6. INMATE/WARD TELEPHONE SYSTEM SERVICES

The Inmate/Ward Telephone System (IWTS) services specified herein will provide the CDCR facilities with collect, advance pay, and prepaid local, IntraLATA, InterLATA, Interstate, and International telecommunications services for inmates and wards. The IWTS service will also provide CDCR with effective investigative tools and a method of tracking and reporting phone usage.

The Prime Contractor will be responsible for a complete and all-inclusive service offering at no cost to the State. The Prime Contractor's revenue to support all the requirements in this Contract will be derived only from the one-time setup fee for prepaid accounts, per use transaction fee with AdvancePay One Calls, and the "per-conversation minute" rate billed to the called parties. Reference Exhibit J Advance Pay Options for an explanation of the prepaid account on-time transaction and AdvancePay One Call transaction fees.

## 7. MANAGED ACCESS SYSTEM/CELL PHONE INTERDICTION SOLUTIONS SERVICES

The Managed Access System (MAS) services will provide the CDCR with complete 24-hour, continuous blocking of all unauthorized cellular wireless communications within the defined scope of each facility. However, the MAS shall permit processing of 9-1-1 Emergency Telephone System (9-1-1 ETS) calls from all cellular wireless communication devices as required by federal, state, and local laws and regulations. Concurrently, the MAS will allow full transmission functionality of authorized cellular devices operating in the same coverage areas.

The Cell Phone Interdiction Solutions services will provide CDCR with tools and devices for detection, surveillance, extraction, and analysis of all unauthorized cellular wireless communication devices and other contraband items to help eradicate the contraband cell phones in the Adult facilities.

The Prime Contractor will be responsible for a complete and all-inclusive service offering for both MAS and CIS at no cost to the State.

## 8. CONTRACT ADMINISTRATION FEE

After completion of the Transition-In phase and for the remaining term of the Contract, an annual Contract Administration Fee of $800,000 will be payable by the Prime Contractor, in monthly increments of $66,666.66 due on the last day of each month in arrears via wire transfer to cover the State contract management responsibilities and services. The State will provide the Prime Contractor the name and account information for the purpose of receiving these funds.

Payments that are late by more than 30 calendar days without prior approval of the State representative will be subject to a financial penalty of one and one-half percent (1.5%) per month of the administration fee payment balance due. Successive late payments or late submission of reports will be subject to service level agreement remedies as described in Section 6.12.4, IWTS Administrative Service Level Agreements.

During transition periods (in and out) of the Contract, a pro-rated portion of the $800,000 Contract Administrative Fee will be assessed on a per-site basis. A pro-rated amount of the Contract Administration Fee will be applied to each site to determine the site's portion of the annual fee. The pro-rated Contract Administration Fee will be calculated from the site total conversation minutes as a percentage of the total contract conversation minutes from the State fiscal year baseline 2010, as identified in Exhibit 6-L2, CDCR 2010 IWTS Call Volume by Facility. The Contract Administration Fee will be due within 30 calendar days of written acceptance, by the CDCR Operations Manager, after successful cutover of the site. This pro-rated Contract Administration Fee will be paid monthly, in arrears, until all CDCR IWTS facilities are successfully cutover.

The following example, including Table SOW-1 Contract Administration Fee Calculation – Site specific Pro-rated Fee, reflects the calculation of the Contract Administration Fee during transition phases.

| Table SOW-1 Contract Administration Fee Calculation – Site specific Pro-rated Fee | | **Acronym** |
|---:|---|---|
| $800,000 | Total Contract Administration Fee | TCAF |
| 5,276,444 | 2010 IWTS Call Volume Location Annual Total Minutes<br>Example: Avenal State Prison (ASP) | LATM |
| 99,666,347 | 2010 IWTS Statewide Annual Total Minutes | SATM |
| 5.2941% | Site Percentage (for Avenal of 2010 Statewide Annual Total Minutes) | SP |
| $42,352.80 | Site Annual Fee Portion (of Annual $800,000 Administrative Fee for ASP) | SAFP |
| $3,529.40 | Site Monthly Fee Portion (for ASP) | SMFP |

1) Divide the 2010 IWTS Call Volume Location Annual Total Minutes (LATM) for ASP by the 2010 IWTS Statewide Annual Total Minutes (SATM), to determine the ASP Site Percentage (SP).

   LATM divided by SATM = SP

2) Multiply the $800,000 Total Contract Administration Fee (TCAF) by the SP to determine the Site's Annual Fee Portion (SAFP) of the Contract Administration Fee.

   TCAF x SP = SAFP

3) Divide the SAFP by 12 to determine the Site's Monthly Portion (SMFP) of the Contract Administration Fee.

   SAFP divided by 12 = SMFP

## 9. NONREIMBURSEMENT OF ADDITIONAL COSTS

The State will not pay the Prime Contractor any lump sum or other start-up expenses for services, nor for any expenses incurred in the preparation of a Bid, even though the Prime Contractor shall be obligated to begin some aspects of performance immediately after Contract award and before in-service/cutover, including preparation, implementation, coordination and reporting necessary to ensure that full IWTS/MAS/CIS services shall be ready by the required in-service cutover date. The State will not pay the Prime Contractor any lump sum or other expenses for close-down or termination costs at the time the Prime Contractor ceases to provide service under the Contract.

## 10. SERVICE LEVEL AGREEMENTS

Section 6.12, IWTS Service Level Agreements (SLAs); Section 6.23, MAS Service Level Agreements; Section 6.25.17, CIS Service Level Agreements; detail the benchmarks of service that the Prime Contractor is expected to maintain for the IWTS, MAS, and CIS services throughout the term of the Contract and their appropriate remedies. The Prime Contractor's failure to meet the Service Levels may result in the lowering of the per-Conversation Minute rates as detailed in SOW Section 11, Annual Run Rate Cost Adjustments.

The State will perform a quarterly review of the SLA reports provided by the Prime Contractor.

## 11. ANNUAL RUN RATE COST ADJUSTMENTS

On an annual basis, the State will conduct an analysis of the previous year's Conversation Minutes (CM) and Service Level Agreement Rights and Remedies Minutes (SLARRM) to determine if reductions to established Adult per Conversation Minute Rates (ACMR) and Youth per Conversation Minute Rates (YCMR) should be applied.

The annual CM for any given period is defined as the IWTS Call Volume expressed in minutes.

The SLARRM for any given period is the total of the Rights and Remedies Minutes reflecting SLA violations for both IWTS (ISLARRM) and MAS (MSLARRM). The monthly SLA Summary Report reflects the "penalty minutes" assessed and applied toward the MSLARRM and ISLARMM totals. Rights and Remedy minutes must be reported within 60 calendar days from the last day of the month in which the SLA objective was missed.

The IWTS annual CM and ISLARRM will be totaled at the end of each calendar year commencing after acceptance of IWTS transition. The MAS MSLARRM will be totaled at the end of each calendar year commencing after the State's acceptance of MAS implementation at each site.

Rate reductions will be applied as a result of the IWTS/MAS Run Rate Method. The results of this method calculation will be applied to all Adult and Youth per-Conversation Minute Rates throughout the remaining term of the Contract. Upon written notification by the State, rate reductions must be implemented by the Prime Contractor within 60 calendar days.

### 11.1 IWTS/MAS/CIS Run Rate Method

On an annual basis, the Prime Contractor will reduce the ACMR and YCMR by five percent (5%) if the SLARRM exceeds the Threshold Percentage (TP) of 1 percent (1%) of the annual Conversation Minutes (CM) of the previous calendar year.

Table SOW-2 Rate Reduction Calculation Example.

| Run Rate Component | Acronym | Previous Year* | New Rates* |
|---|---|---|---|
| Annual Conversation Minutes | CM | 105,000,000 | |
| IWTS Service Level Agreement Rights and Remedies Minutes | ISLARRM | 1,300,000 | |
| MAS Service Level Agreement Rights and Remedies Minutes | MSLARRM | 1,000,000 | |
| CIS Service Level Agreement Rights and Remedies Minutes | MSLARRM | 500,000 | |
| Total | SLARRM | 2,800,000 | |
| Threshold Percentage of 1% | TP | 1% | |
| Youth per Conversation Minute Rates (per 15-minute call) Local Call | YCMR | $0.420 | **$0.399** |
| Adult per Conversation Minute Rates (per 15-minute call) Local Call | ACMR | $1.440 | **$1.368** |

*The totals and rates used in the table are for example purposes only.

Example:

Combine ISLARRM + MSLARRM = Annual SLARRM
If SLARRM / CM > 1% (TP), then apply the rate reduction adjustment calculation.
1,300,000 + 1,000,000 + 500,000 = 2,800,000
2,800,000 / 105,000,000 = 0.0267
0.0267 > 0.01

Calculate percent by multiplying the decimal by 100: 0.0267 X 100 = 2.67%
(2.67% is greater than 1%)

IF TP is greater than 1%; then calculate new YCMR and ACMR:
New YCMR = YCMR - 5%
New YCMR = $0.420 - ($0.420 X 0.05)

New YCMR = $0.399

New ACMR = ACMR - 5%
New ACMR = $1.440 - ($1.440 X 0.05)
New ACMR = $1.368

## 12. DEFINITIONS

Definitions for the terms used in this Contract are provided in Appendix C, Glossary of Terms.

## 13. CDCR FACILITIES AND IWTS EQUIPMENT

The quantities of components that are anticipated to be deployed at each CDCR facility are detailed in Section 6 Exhibits that are specifically referenced in this section. The anticipated number of facilities and IWTS related equipment may increase or decrease within the term of the Contract based upon activation or deactivation of facilities to accommodate inmate population changes and/or changes in CDCR operations and programs.

### 13.1 Adult Facilities

1) Exhibit 6-C1, Adult Institution Locations, includes the CDCR facilities' names, addresses, and telephone numbers. Exhibit 6-C2, Adult Institutions' IWTS Anticipated Equipment, includes the detail of the quantities and types of IWTS equipment at the adult institutions.
2) Exhibit 6-D1, CDF/CDCR Adult Camp IWTS Locations, includes the camp names, addresses, and telephone numbers. Exhibit 6-D2, CDF/CDCR Adult Camps' IWTS Anticipated Equipment, includes the detail of the quantities and types of IWTS equipment at the adult camps.
3) Exhibit 6-E1, Additional Adult Facility IWTS Locations, includes the names, addresses, and telephone numbers of the Community Correctional Facilities (CCFs) and Female Offender Programs (FOPs) that are privately operated and have custody oversight for CDCR inmates. Exhibit 6-E2, Additional Adult Facilities' IWTS Anticipated Equipment, include the detail of the quantities and types of IWTS equipment installed at these locations.
4) Exhibit 6-F1, New Adult Facility IWTS Locations Anticipated, includes the names, addresses, and telephone numbers of future locations that include CDCR facilities that are anticipated or in various design, construction, or conversion stages. Exhibit 6-F2, New Adult Facilities' IWTS Anticipated Equipment includes the detail of the quantities and types of IWTS equipment at these locations.

### 13.2 Youth Facilities

Exhibit 6-G1, Youth Facility Locations, includes the names, addresses, and telephone numbers of the youth facilities. Exhibit 6-G2, Youth Facilities' IWTS Anticipated Equipment includes the detail of the quantities and type of IWTS equipment at the youth facilities. Youth facilities will record all calls and may monitor ward calls. This change may require IWTS workstations installed at some youth facilities.

### 13.3 CDCR Field Offices

CDCR Field Offices will not require on-site equipment. The CDCR Authorized staff will perform the IWTS Investigative Workstation Functionality and IWTS Tools and Reports by using a State computer to access the Prime Contractor hosted web-based IWTS application. The Prime Contractor shall provide support with access to the web-based IWTS application, as needed.

### 13.4 Replacement of All IWTS Equipment

All IWTS equipment (with the exception of the state-owned enclosures refer to Section 6.3.2.4, IWTS Telephone Enclosures that Include Booths, Wall and/or Pedestals) will be replaced with new equipment in the IWTS/MAS Contract. During Transition-In, the Prime Contractor will replace all of the IWTS equipment components that are described in the Exhibits in this section. The CDCR Operations Manager will verify that the IWTS equipment provided is consistent with the Section 6, Technical Requirements.

## 14. IWTS CALL CONTROL SYSTEM CATEGORIES

The IWTS shall provide the ability to create five (5) categories for Call Control. A description of each category is provided in Exhibit 6-J, Call Control System Categories. These categories are defined by their functionality, related equipment, and storage of recordings for the adult and youth facilities. The five (5) Call Control system categories include: Adult Institutions, Adult Camps, Adult CCF and FOP Locations, Youth Facilities, and Field Offices.

## 15. MAS/CIS LOCATIONS

The MAS shall be installed at the CDCR Adult Institutions and Youth Facilities. A listing of the current CDCR facilities is provided in Exhibit 6-O, Adult Institution MAS Locations. .

The CIS shall be installed at CDCR Adult Institutions. A listing of the anticipated CDCR facilities is provided in Exhibit 6-S1, Cell Phone Interdiction Solutions Facilities. In addition, Forensic Investigative Extraction and Analysis tools shall be provided at CDCR Headquarters as part of the CIS.

## 16. IWTS COLLECT AND PREPAID RATES

The IWTS/MAS Contract, Attachment 7, Cost Worksheets, reflects the Prime Contractor's collect and prepaid rates for the term of this Contract including optional years. These rates will be posted on the State's web site at http://www.dts.ca.gov/stnd/calnet-inmate-ward.asp and Prime Contractor's public portal web site for the public to reference.

The CDCR call volume summaries are detailed in Exhibit 6-K1, CDCR 2008 IWTS Call Volume by Call Type, Exhibit 6-K2, CDCR 2009 IWTS Call Volume by Call Type, Exhibit 6-K3, CDCR 2010 IWTS Call Volume by Call Type, Exhibit 6-L1, CDCR 2009 IWTS Call Volume by Facility, and Exhibit 6-L2, CDCR 2010 IWTS Call Volume by Facility. Additionally, International call volume summaries are detailed in Exhibit 6-M1, CDCR 2009 IWTS International Call Volume by Country by Month, and Exhibit 6-M2, CDCR 2010 IWTS International Call Volume by Country by Month. The summary and quantities are included for historical purposes. The CDCR facilities may increase or decrease based upon operational changes which may impact changes to the call volume. Call volumes are not expected to differ appreciably in the future, but the Prime Contractor will accept full risk with respect to State required deployment requirements and billable call volumes. Dependent on the needs of the State and at the State's request, the Prime Contractor will provide additional (or less) services as defined in this Contract during the term of the IWTS/MAS Contract period, including optional years, without a change in rates.

## 17. STATE RESPONSIBILITIES

### 17.1 State Physical Plant Infrastructure

1) For IWTS services - The State retains sole responsibility for performing any changes to installed physical plant infrastructure components such as wiring and conduits.

2) For MAS services - The State shall have no responsibility for the physical plant infrastructure components such as wiring and conduits.

3) For CIS services - The State retains sole responsibility for performing any changes to installed physical plant infrastructure components such as wiring and conduits.

### 17.2 Implementation of New and Existing IWTS/MAS/CIS Services

The State reserves the right, at its sole discretion, to restrict, delay, halt or discontinue all or part of any implementation of new or existing IWTS/MAS/CIS services if a mandatory technical requirement included in Section 6, Technical Requirements, fails to function. If this occurs, within three (3) business days after the State is aware of the defect, the State will document and provide the Prime Contractor written notification of the specific requirement. The Prime Contractor will have three (3) business days to provide a response that would include identification of corrective action and a proposed timeline. Upon receipt, the State will review the Prime Contractor's response and schedule a meeting with the Prime Contractor to discuss and finalize the corrective action and timeline.

### 17.3 Coordination

The State will retain core technology management functions for strategic planning, quality assurance, and contract management. The State will retain authority over specific IWTS/MAS service functions.

### 17.4 Service Support and Maintenance Responsibilities

1) Provide access to Prime Contractor's equipment at CDCR facilities;

2) Coordinate one-time gate clearance(s), in SOW, Exhibit A, Gate Clearance Informational and Approval Sheet; SOW, Exhibit C, Primary Laws, Rules, and Regulations Regarding Conduct and Association with State Prison Inmates and all other responsibilities as described throughout this Contract, and annual CDCR identification badges for Prime Contractor's staff to access the CDCR facilities;

3) Provide Prime Contractor with a list of CDCR personnel authorized to call the Help Desk to report trouble tickets. This list shall be updated twice a year or as needed; and,

4) Provide the concrete pad for IWTS telephone enclosures or pedestals.

## 18. TECHNOLOGY UPGRADE AND MODIFICATION APPROVAL

The State retains the right to accept or reject any Prime Contractor proposed technology upgrade, modification, or enhancement plan that changes the IWTS/MAS serviced infrastructure.

## 19. FUTURE BUSINESS PROCESS REENGINEERING

It is anticipated that the Prime Contractor will propose, initiate, and conduct technology infrastructure changes that result in business process reengineering efforts at the State. The State will retain primary responsibility and authority over approving these efforts and ensuring that performance metrics (including before and after) are accurately and appropriately developed.

## 20. MOVES, ADDS, AND CHANGES OF THE IWTS/MAS/CIS EQUIPMENT

The CDCR Operations Manager will be responsible for coordination of all moves, adds, and changes of the IWTS/MAS/CIS equipment. The Prime Contractor will be required to perform a site survey and prepare a site survey report that includes digital photos of the existing locations to document changes, as well as identify the CDCR and Prime Contractor's Responsibilities. The CDCR Operations Manager will review and approve the site survey report before it is shared with the CDCR facility. Refer to SOW, Exhibit D, IWTS Work Authorization Process and Form and SOW, Exhibit E, MAS/CIS Work Authorization Process and Form. The CDCR Operations Manager will direct the Prime Contractor to install, relocate, and deactivate telephones at the State's discretion regardless of the call volume and usage. The timeframes for the coordination include:

1) New Activation - Prime Contractor will have 60 calendar days from the written notification received from CDCR Operations Manager to order circuits, procure equipment, and install a new facility;
2) Additional Equipment at an Existing Facility - Prime Contractor will have 45 calendar days from the written notification received from CDCR Operations Manager to procure equipment and install at an existing facility that will require additional IWTS equipment; and,
3) Relocation of Equipment at an Existing Facility - Prime Contractor will have 30 calendar days from the written notification received from CDCR Operations Manager to deactivate and remove equipment installed at an existing facility.

## 21. CHANGE REQUEST PROCESS

The Prime Contractor shall submit a written request to the CDCR Operations Manager using, SOW, Exhibit F, Contract Change Request when a change is being requested.

The Prime Contractor shall submit this form for any positive or negative impact to the scope of the project. The form shall be submitted with estimated scope impact or project time impact in an email to the CDCR Operations Manager. The Prime Contractor may proceed with the change request once CDCR approves and responds.

## 22. REQUEST FOR INFORMATION

If additional detailed site specific information is required for engineering the IWTS and MAS Services, the Prime Contractor shall submit a written request to the CDCR Operations Manager using SOW, Exhibit G, Request For Information California Department of Corrections and Rehabilitation. The CDCR Operations Manager will then evaluate the request to ensure that there is no risk to security before releasing the information.

Any request for CDCR Data/Information will require the submission of SOW, Exhibit H, Information Access and Security Agreement.

***(INTENTIONALLY BLANK)***

## 23. EXHIBITS

### SOW EXHIBIT-A GATE CLEARANCE INFORMATIONAL & APPROVAL SHEET

(STAFF ONLY)

Requestor: ____________________ Department: ____________________ Extension: __________________

Division Head Authorization ________________________________________Date: ______________________
(Print and Sign)

Purpose of Entry: ____________________________________________________________________________

Date(s)______________________ Time: ____________________Duration ___________________________

Escort:_______________________________________________________________________________________

Type of Authorization Requested (Check One): □Gate Clearance □State ID Card (Contract)

Name of Company: ____________________________________________________________________________

Name_________________________________________________________________________________________
(Last) (First) (Middle)

Area Code and Phone Number Day: _______________________ Night:_______________________________________

Date of Birth: Month: ________ Day: ________ Year: ________ Gender: □Female □Male

Driver's License Number: _________________ State: _______ Social Security Number:_____________________

I also have been known by these names: ______________________________________________________________

I visit an inmate in a Correctional Institution: □Yes □No

I have been arrested and/or convicted of a crime: □Yes (attach sheet if more than 2) □ No

| Offense | Approximate Date | Disposition |
|---|---|---|
| | | |
| | | |

Are you a former inmate? □ Yes □ No

**NOTE THE FOLLOWING CONDITIONS/RESTRICTIONS**

If you are on parole, probation or have been incarcerated, you must provide written consent from your supervising agency to enter these grounds. If you are under 18 years of age, you must have written, notarized consent provided by your parent or legal guardian and be accompanied by a responsible adult in order to enter these grounds. All questions must be answered! Any omission or falsification on this form shall be considered sufficient reason for denial of access.

The person listed above will only be allowed to enter the designated area(s) and only under employee escort unless otherwise authorized with an Identification Cared. Law Enforcement Personnel will be given authorization to enter grounds upon showing appropriate identification and no security clearance is necessary. A previous clearance is not an automatic approval for future clearances. You must resubmit a request if any clearance has expired.

**Signature of Applicant**: _____________________________________ Date: _______________________

CI&I CLEARANCE

□APPROVED □DISAPPPROVED SIGNATURE:_______________________________DATE:______________

***INTENTIONALLY BLANK***

# SOW EXHIBIT-B DIGEST OF LAWS RELATING TO ASSOCIATION WITH INMATES (DELETED)

***(INTENTIONALLY BLANK)***

# SOW EXHIBIT-C PRIMARY LAWS, RULES, AND REGULATIONS REGARDING CONDUCT AND ASSOCIATION WITH STATE PRISON INMATES

## STATE OF CALIFORNIA

CDC 181 (Rev 5/98)

Individuals who are not employees of the California Department of Corrections and Rehabilitation (CDCR), but who are working in and around inmates who are incarcerated within California's institutions/facilities or camps, are to be apprised of the laws, rules and regulations governing conduct in associating with prison inmates. The following is a summation of pertinent information when non-departmental employees come in contact with prison inmates.

1. Persons who are not employed by CDC, but are engaged in work at any institution/facility or camp must observe and abide by all laws, rules and regulations governing the conduct of their behavior in associating with prison i8nmages. Failure to comply with these guidelines may lead to expulsion from CDC institutions/facilities or camps.
   SOURCE: California Penal Code (PC) Sections 5054 and 5058; California Code of Regulations (CCR), Title 15, Sections 3285 and 3415

2. CDCR does not recognize hostages for bargaining purposed. CDCR has a "NO HOSTAGE" policy and all prison inmates, visitors, and employees shall be made aware of this.
   SOURCE: PC Sections 5054 and 5058; CCR, Title 15, Section 3304

3. All persons entering onto institution/facility or camp grounds consent to a search of their person, property or vehicle at any time. Refusal by individuals to submit to a search of their person, property or vehicle may be a cause for denial of access to the premises.
   SOURCE: PC Sections 2601, 5054 and 5058; CCR, Title 15, Sections 3173 and 3288

4. Persons normally permitted to enter an institution/ facility or camp may be barred, for cause, by the CDCR Director, Warden and/or Regional Parole Administrator.
   SOURCE: PC Sections 5054 and 5058; CCR, Title 15, Section 3176 (a)

5. It is illegal for an individual who has been previously convicted of a felony offense to enter into CDCR institutions/facilities or camps without the prior approval of the Warden. It is also illegal for an individual to enter onto these premises for unauthorized purposes or to refuse to leave said premises when requested to do so. Failure to comply with this provision could lead to prosecution.
   SOURCE: PC Sections 602, 4570.5 and 4571; CCR, Title 15, Sections 3173 and 3289

6. Encouraging and/or assisting prison inmates to escape is a crime. It is illegal to bring firearms, deadly weapons, explosives, tear gas, drugs or drug paraphernalia on CDCR institutions/facilities or camp premises. It is illegal to give prison inmates firearms, explosives, alcoholic beverages, narcotics, or any drug or drug paraphernalia, including cocaine or marijuana.
   SOURCE: PC Sections 2772, 2790, 4533, 4535, 4550, 4573, 4573.5, 4573.6 and 4574

7. It is illegal to give or take letters from prison inmates without the authorization of the Warden. It is also illegal to give or receive any type of gift and/or gratuities from prison inmates.
   SOURCE: PC Sections 2540, 2541 and 4570; CCR, Title 15, Sections 3010, 3399, 3401, 3424 and 3425

8. In an emergency situation the visiting program and other program activities may be suspended.
   SOURCE: PC Section 2601; CCR, Title 15, Section 3383

9. For security reasons, visitors must not wear clothing that in any way resembles state issued prison inmate clothing (blue denim shirts, blue denim pants).
   SOURCE: CCR, Title 15, Section 3171 (b) (3)

10. Interviews with SPECIFIC INMATES are not permitted. Conspiring with an inmate to circumvent policy and/or regulations constitutes a rule violation that may result in appropriate legal action.
    SOURCE: CCR, Title 15, Section 3261.5, 3315 (3) (W), and 3177.

I HEREBY CERTIFY AND ACKNOLEDGE I HAVE READ THE ABOVE AND FULLY UNDERSTAND THE IMPLICATIONS REGARDING MY CONDUCT AND ASSOCIATION WITH PRISON INMATES. I ALSO UNDERSTAND VIOLATION OF ANY OF THE ABOVE COULD RESULT IN EXPULSION FROM A CDC INSTITUTION/FACILITY OR CAMP WITH THE POSSIBILITY OF CRIMINAL PROSECUTION.

| | | |
|---|---|---|
| VISITOR'S NAME AND TITLE (Print) | VISITOR'S SIGNATURE | DATE SIGNED |

DISTRIBUTION: Original – Assistant Director, Communications Canary – Warden's Office Pink - Visitor

*(INTENTIONALLY BLANK)*

# SOW EXHIBIT-D IWTS WORK AUTHORIZATION PROCESS AND FORM

## Prime Contractor Process Guidelines

**Approach:** The Work Authorization Process is being used to submit Inmate/Ward Telephone System (IWTS) non-billable work orders to the Prime Contractor and track the work order progress. The non-billable work orders will be generated by the State for IWTS moves, adds, and changes. The California Department of Corrections and Rehabilitation (CDCR) Operations Manager or designee will coordinate and monitor work performance by the Prime Contractor.

**Contacts:**

| ***Role*** | ***Name*** | ***Email*** | **Phone#** |
|---|---|---|---|
| CDCR Operations Manager | TBD | TBD | TBD |
| STND CMS CM | TBD | TBD | TBD |
| STND CMS POC | TBD | TBD | TBD |
| STND CMS Backup POC | TBD | TBD | TBD |
| STND CEU POC | TBD | TBD | TBD |
| Contractor POC | TBD | TBD | TBD |

**Process:** If any issues develop during the IWTS Work Authorization Process, the Statewide Telecommunications and Network Division, Contract Management Section Point of Contact (STND CMS POC) immediately escalates the issue(s), via e-mail, to the STND CMS CM and copies the CDCR Operations Manager or designee, CMS Backup POC, and STND CALNET Engineering Unit (CEU) POC on all correspondence regarding these issues.

Contractor Review & Signature

A Work Authorization detailing the scope of work will be e-mailed to the Prime Contractor POC for approval of the Work Authorization Request. The approved Work Authorization Request is then scanned and e-mailed back to the CDCR Operations Manager or designee.

Work Coordination & Performance

The CDCR Operations Manager or designee and the Prime Contractor POC will work together to complete the scope of work described in the IWTS Work Authorization. In most cases, the CDCR Operations Manager or designee will be on site to confirm the work has been completed. In cases where the CDCR Operations Manager is not on site, the CDCR Operations Manager or designee will work with the CDCR site contact to verify work has been completed. The original Work Authorization Request is signed and mailed to STND CMS POC at the following address:

California Technology Agency/OTECH
STND-Contract Management Section
Attention: TBD
P.O. Box 1810, MS Y-13
Rancho Cordova, CA 95741-1810

If additional work is identified as being needed after the IWTS Work Authorization Request has been signed and the Prime Contractor is on site, the CDCR Operations Manager or designee will provide a Change Request to Work Authorization, which has been signed by the Contractor on site, referencing the original Work Authorization Number (WA#) and additional work performed. This Change Request to Work Authorization will be scanned by the CDCR Operations Manager and e-mailed to the STND CMS POC. The Original will be mailed to STND CMS POC.

## Work Authorization Close-out

Upon completion of the project, the STND CMS State CM signs the IWTS Work Authorization Request and the STND CMS POC e-mails the completed IWTS Work Authorization to Contractor POC.

SOW EXHIBIT-D IWTS WORK AUTHORIZATION PROCESS AND FORM (CONTINUED)

**INMATE/WARD TELEPHONE SYSTEM (IWTS)**
**WORK AUTHORIZATION REQUEST**
**WA #:**

**PROJECT NAME:** **Date:**

**SCOPE OF WORK:**

## SCHEDULED DATES:

Start Date:

Completion Date:

## CDCR-HQ PROJECT MANAGER:

Name:

Email:

Phone:

## CONTRACTOR POINT OF CONTACT:

Name:

Email:

Phone:

## INITIATION OF PROJECT SIGNATURE APPROVALS:

STND Contract Manager Date

CDCR-HQ Project Manager Date

Contractor Project Manager Date (Clock starts )

## COMPLETION OF PROJECT SIGNATURE APPROVALS:

These tasks were performed in accordance with this Work Authorization and the provisions of Contract # DGS-IFB-11-126805.

CDCR-HQ Project Manager Date

Contractor Project Manager Date

STND Contract Manager Date

***INTENTIONALLY BLANK***

## SOW EXHIBIT-E MAS/CIS WORK AUTHORIZATION PROCESS AND FORM

### PRIME CONTRACTOR PROCESS GUIDELINES

**Approach:** The Work Authorization Process is being used to submit Managed Access System (MAS) and Cell Phone Interdiction Solutions (CIS) non-billable work orders to the Prime Contractor and track the work order progress. The non-billable work orders will be generated by the State for MAS/CIS moves, adds, and changes. The California Department of Corrections and Rehabilitation (CDCR) Operations Manager or designee will coordinate and monitor work performance by the Prime Contractor.

**Contacts:**

| ***Role*** | ***Name*** | ***Email*** | ***Phone#*** |
|---|---|---|---|
| CDCR Operations Manager | TBD | TBD | TBD |
| STND CMS CM | TBD | TBD | TBD |
| STND CMS POC | TBD | TBD | TBD |
| STND CMS Backup POC | TBD | TBD | TBD |
| STND CEU POC | TBD | TBD | TBD |
| Contractor POC | TBD | TBD | TBD |

**Process:** If any issues develop during the MAS Work Authorization Process, the Statewide Telecommunications and Network Division, Contract Management Section Point of Contact (STND CMS POC) immediately escalates the issue(s), via e-mail, to the STND CMS CM and copies the CDCR Operations Manager or designee, CMS Backup POC, and STND CALNET Engineering Unit (CEU) POC on all correspondence regarding these issues.

Contractor Review & Signature

A Work Authorization detailing the scope of work will be e-mailed to the Prime Contractor POC for approval of the Work Authorization Request. The approved Work Authorization Request is then scanned and e-mailed back to the CDCR Operations Manager or designee.

Work Coordination & Performance

The CDCR Operations Manager or designee and the Prime Contractor POC will work together to complete the scope of work described in the MAS/CIS Work Authorization. In most cases, the CDCR Operations Manager or designee will be on site to confirm the work has been completed. In cases where the CDCR Operations Manager is not on site, the CDCR Operations Manager or designee will work with the CDCR site contact to verify work has been completed. The original Work Authorization Request is signed and mailed to STND CMS POC at the following address:

California Department of Technology
STND-Contract Management Section
Attention: TBD
P.O. Box 1810, MS Y-13
Rancho Cordova, CA 95741-1810

If additional work is identified as being needed after the MAS/CIS Work Authorization Request has been signed and the Prime Contractor is on site, the CDCR Operations Manager or designee will provide a Change Request to Work Authorization, which has been signed by the Contractor on site, referencing the original Work Authorization Number (WA#) and additional work performed. This Change Request to Work Authorization will be scanned by the CDCR Operations Manager and e-mailed to the STND CMS POC. The Original will be mailed to STND CMS POC.

## SOW EXHIBIT-E MAS/CIS WORK AUTHORIZATION PROCESS AND FORM (CONTINUED)

Work Authorization Close-out

Upon completion of the project, the STND CMS State CM signs the MAS/CIS Work Authorization Request and the STND CMS POC e-mails the completed MAS/CIS Work Authorization to Contractor POC.

## MANAGED ACCESS SYSTEM (MAS)/CELL PHONE INTERDICTION SOLUTIONS (CIS)
## NEW WORK AUTHORIZATION REQUEST
## WA #:

**PROJECT NAME:** **Date:**

**SCOPE OF WORK:**

## SCHEDULED DATES:

Start Date:

Completion Date:

## CDCR-HQ PROJECT MANAGER:

Name:

Email:

Phone:

## CONTRACTOR POINT OF CONTACT:

Name:

Email:

Phone:

## INITIATION OF PROJECT SIGNATURE APPROVALS:

STND Contract Manager Date

CDCR-HQ Project Manager Date

Contractor Project Manager Date (Clock starts )

## COMPLETION OF PROJECT SIGNATURE APPROVALS:

These tasks were performed in accordance with this Work Authorization and the provisions of Contract # DGS-IFB-11-126805.

CDCR-HQ Project Manager Date

Contractor Project Manager Date

STND Contract Manager Date

***INTENTIONALLY BLANK***

# SOW EXHIBIT-F CONTRACT CHANGE REQUEST

STATE OF CALIFORNIA—YOUTH AND ADULT CORRECTIONAL AGENCY Edmund G. Brown, Jr., *Governor*

**DEPARTMENT OF CORRECTIONS AND REHABILITATION**
Enterprise Information Services
P.O. Box 942883
Sacramento, CA 94283-0001

**CDCR FACILITY:** **DATE:**

**CDCR IWTS/MAS/CIS OPERATIONS MANAGER:** **NUMBER:**

**Change Description**

**Reason for Change:**

**Impacts:**

- **Schedule:** ____________________
- **Design Intent:** ____________________
- **Other:** ____________________

**Initiated by:** Prime Contractor Date ____________________
□ Recommended
□ Not Recommended ____________________ Date ____________________

□ Recommended
□ Not Recommended ____________________ Date ____________________

□ Approved
□ Not Approved ____________________ Date ____________________
□ **Additional Departmental Review Required**

***INTENTIONALLY BLANK***

# SOW EXHIBIT-G REQUEST FOR INFORMATION CALIFORNIA DEPARTMENT OF CORRECTIONS AND REHABILITATION

**TO**:

Facility Name ______________________

Phase Number

**FROM**:

**SUBJECT**:___________________________________

**BUILDING/ROOM**:______________________________ **DATE ISSUED**: _______________________________

**DWG. REF.**_________________ **SPEC REF.**________**DATERESPONSE REQUIRED**: _ ________________

**QUESTION/PROPOSED SOLUTION**: Attached Sheets: YES NO

**POTENTIAL IMPACT**
( ) SCHED ( ) LABOR ( ) MTR'L
( ) NO IMPACT ( ) OTHER

Contractor Rep.________________________

Reviewed by CM:________________________ Date:_______________ Sent To:__________________

**REPLY**: Attached Sheets: YES NO

Responding Firm:_____________________________ By:__________________Date:_______________

Response Reviewed and Forwarded by CM:__________________________ Date:__________________

***INTENTIONALLY BLANK***

# SOW EXHIBIT-H INFORMATION ACCESS AND SECURITY AGREEMENT

**The State Administrative Manual (SAM) Section 4841.2 requires that State agencies acquire written agreements with non-State entities (for example, vendors, consultants, researchers, federal and local government entities, or other state entities) before agencies allow access to State data. This agreement fulfills the requirement for query access requests from all non-CDCR entities, including non-State entities. Alternate agreements are required for all other access requests, including requests to transmit and store CDCR data. Refer to Department Operations Manual (DOM), §§ 49020.9 and 49020.10.**

□ New Request □ Renewal Request

Requestor: ______________________ Company/Affiliation: ______________________
Title: ______________________ E-mail: ______________________
Telephone: ______________________ Fax No.: ______________________
Contract/Agreement No. (if applicable): ______________________

I agree to the following terms and conditions:

- I shall comply with all State policies and laws regarding use of State information resources and data.
- I agree not to store, distribute, or share information obtained through this agreement and access authorization in any way without prior written approval from California Department of Corrections and Rehabilitation (CDCR) and shall hold this information in strict confidence.
- I agree to use CDCR information and information access for authorized purposes only.
- I agree to exercise all precautions necessary to assure the protection of CDCR information in my care from unauthorized disclosure, access, modification, and destruction.
- I agree to use my user ID and password to access this system only while completing my assigned duties. I understand that my user ID and password may not be shared with or used by any other person.
- I agree to notify CDCR promptly if information obtained through this agreement is compromised, lost, or stolen. This includes unauthorized use of the CDCR-provided user ID and password.
- I understand that unauthorized access or disclosure of information provided to me by CDCR may be a public offense punishable under Section 502 of the California Penal Code.
- I understand that CDCR may monitor my access at any time, with or without notice, for the purpose of ensuring compliance with agreement.
- I also understand that this agreement must be renewed annually each year that I am provided access to CDCR information. I further acknowledge that I have received and reviewed a copy of the attached CDCR Information Security Policies.

**Requestor's Signature**:

______________________ ______________________
(Name) (Date)

**For CDCR Use Only**

SYSTEM ACCESS AUTHORIZED BY: ______________________
SYSTEM TO BE ACCESSED: ______________________
ASSIGNED USER ID: ______________________
ACCESS ACCOUNT CREATED BY: ______________________

The data to be accessed contains confidential or personal information: □ Yes □ No

DISTRIBUTION: Original-File / Copy-Requestor

SOW EXHIBIT-I CDCR IT Change Management Policy Documentation Guidelines

# California Department of Corrections

## IT Change Management Policy Documentation Guidelines

## TABLE OF CONTENTS

## LIST OF TABLES

## LIST OF FIGURES

# 1.0 Governance Introduction

## 1.1 CDCR Mission

The documentation of CDCR IT change management (ITCM) governance should provide clear guidance for everyone to follow when IT introduces a change to the production environment that could affect client service. The change management process is intended to manage any change that might prevent a system from behaving as the client expects. For example, the ITCM process supports the delivery of services as stated in the service-level agreement (SLA) between IT and the client.

Typically, the ITCM process will offer process guidance to all situations or proposed alterations to an IT service. Alterations to an IT service require a change record that IT can track and retain for future reference. Documentation and standardized procedural control provide protection for any change that may have complications, and provide for each change to be addressed in a consistent procedural manner.

## 1.2 Process Goals

The fundamental strategy for ITCM process governance is to ensure that IT implements all changes without any negative impact on customer service. Sample objectives include:

Identify and apply best practices in defining common processes for change throughout an organization

Develop common change management processes within an organization, including roles and responsibilities by functional group and the governance group for managing strategic direction

Allow change, while maintaining or improving system availability

Determine whether the amount of lead time affects the success or failure of non-disruptive changes

When lead time is important, identify sensitive types and volumes of changes to reduce disruptions

Reduce the number of changes requiring "back-out" due to inadequate preparation or defects

Provide complete change documentation to shorten problem determination risk time

Determine a better method of identifying and categorizing changes into levels of risk

Display the number and types of changes planned in the short and long term

Increase the accuracy of predictions regarding the impact of change

Ensure that every change record has technical and management accountability to provide a compliance audit trail

Establish a process to ensure that change requests are consistently reviewed for technical merit and business readiness, while allowing for flexibility based on business needs

Avoid conflicts by managed scheduling

Audit change activity and understand the reasons for failing to comply with processes

### 1.3 Objectives

To support the goals identified in Section 1.2, the following SMART objectives have been defined (SMART is an acronym that can be used to form more-precise objectives: specific scope, measurable or observable, actionable, relevant and time-bound:

### 2.0 Short-Term — Within Six Months:

Reduce failed changes on critical IT services by 10% in three months

Reduce lost revenue caused by failed changes on the order entry website by 50% in three months

Reduce the change cycle time for normal changes by 5% in two months

### 3.0 Longer-Term — Longer Than Six Months:

Integrate all IT external service providers (ESPs) into the change process within 12 months

### 3.1 Scope

The process applies to any IT asset or configuration item (CI) in the production environment, such as:

A database administrator reorganizing a table

A server technician rebooting a server

An application programmer updating code to fix a bug

A project manager scoping server hardware replacements for mission-critical applications

A security manager implementing a new policy for user administration

ITCM includes the tasks necessary for planning, testing and implementing alterations to minimize unwanted effects. The ITCM process integrates with configuration and release management processes.

## 4.0 Change Management Definitions, Roles, Classifications and Procedures

### 4.1 Change Policy Document Management

This section specifies the ownership and document tracking information. It is the official guide and reference for CDCR's 6ITCM process policy and is the definitive source for all IT change activity or revisions to the policy document (see Table 1).

1 Table1. Revision History

| Version | Status | Date | Author/Reviewer | Changes/Justifications |
|---|---|---|---|---|
| 1.00 | | | | |
| 1.01 | | | | |

### 4.1.1 Change Agility Principle

Change management processes and procedures must be flexible and agile enough to accommodate the needs of the business and incident-related emergencies.

**Rationale:**

To enable the change of IT services at a rate that supports the needs of the business, while managing risk.

To support problem management, emergency changes must be provided within the change process.

To expedite change for emergency situations, the change must follow documented processes.

**Implications:**

Emergency changes follow an expedited process flow.

The change manager must track and monitor trends in emergency changes.

Emergency changes must be a low percentage of overall change, because they carry a high level of risk, due to their expedited nature.

**Policies:**

The parties identified in the change request will qualify, authorize and review all changes, including emergency changes.

Designated staff will trigger emergency changes due to high-priority incidents with adequate business justification and authorization.

### 4.1.2 Common Change Management Principle

All changes implemented in the production environment will follow the change management process.

**Rationale:**

To ensure that business risks associated with changes to IT services are properly managed

To ensure regulatory compliance

To ensure that the need to quickly introduce change is balanced with the need to manage risks in accordance with the desires of the business

**Implications:**

Change management must be an overall policy that is adhered to by all groups and resources.

**Policies:**

All teams are responsible for adhering to change management processes.

All changes are handled through the change management processes.

## 4.2 Define Individual Roles and Responsibilities

Identifying who participates, at what point in the process and their level of participation is often referred to as responsible, accountable, consulted, informed (RACI) modeling:

Responsible = participates

Accountable = owns the function

Consulted = advisory role

Informed = notified of work and completion

In addition to helping organizations communicate participation, RACI models help identify gaps/overlaps in participation that often wreak havoc with organizational performance. The many interpretations of the ITCM process evolving to new functional roles are who "owns" specific processes/tasks.

RACI and other personnel models can help define the new roles to support ITCM. In the end, IT needs disciplined people for the successful implementation and execution of ITCM.

2 Table 2. Example: Role RACI Chart for Change Request Documentation Stage

| | **Identify** | **Request** | **Review** | **Create** | **Review** | **Withdraw** | **Record** |
|---|---|---|---|---|---|---|---|
| | Change Requirement | Change | Policies | Submit Change Request (CR) | CR | CR | CR |
| Change Manager | C | C | C | C | A | C | A |
| Change Control Board (CCB) | | | | | | | I |
| Change Coordinator | C | C | C | C | R | C | R |
| Change Implementer | R | R | A | R | R | R | R |

### 4.2.1 Change Process Owner

In general, a process owner is the person with the necessary perspective to design the process to meet the needs of the business. The process owner has the necessary organizational position and political skills to ensure that stakeholders involved with changes to IT Services comply with the ITCM process. For large organizations, the change process owner might be the management team sponsor with change process development and organizational leadership responsibility. In small and midsize businesses, one person can take the change owner and manager roles. The change process owner:

Is accountable for the end-to-end success of the change process

Drives continuous improvement for change management

Liaises with other process owners to establish integration and collaboration

Develops and delivers strategies

Reports to senior leadership per communication plans

### 4.2.2 Change Process Manager

The change process manager is the policy guardian for the change management process, and is responsible for the day-to-day operations of the process. He or she also:

Executes, manages and reviews change management process activities on a weekly basis

Chairs the CCB and the emergency CCB (E-CCB)

Communicates enhancements/modifications to the change management community

Provides training on the change management process

Is responsible for the publication and communication of the schedule of changes

Is responsible for reporting change management metrics with analysis guidance for improvement

Helps identify continual improvement opportunities

### 4.2.3 Change Owner/Requestor

This person initiates a CR, and may reside within the business unit or the IT organization.

### 4.2.4 Change Implementer

5.0 This person is the subject-matter expert in IT who is responsible for the ongoing administration of technologies such as servers, databases and network devices that are within the scope of the ITCM process. As such, this person must follow the ITCM policy that governs how changes are to be managed.

### 5.1.1 Change Coordinator/Administrator

This person is responsible for assisting in CR documentation review for an IT group, department or division. He or she is sometimes referred to as a change coordinator or administrator.

### 5.1.2 Change Control Board (CCB) Member

This person attends scheduled meetings or sends a deputy, and is empowered to make decisions on behalf of the area he or she represents. The CCB may ask participants to take on responsibilities such as a change technical reviewer — a CCB member who provides technical guidance during CCB assessment and authorization stages of one or more CRs. This role usually requires broad business and technical knowledge from the overall IT service to the CI level.

### 5.2 Define CCB and E-CCB Roles and Responsibilities

The CCB is a cross-functional group set up to evaluate change requests for business needs, priorities, costs/benefits, and potential effects to other systems or processes. Typically, the CCB will make recommendations for implementation, further analysis, deferment or cancellation. At a minimum, CCB staffing will include change owner, change manager/agent, representative from configuration management and a change technical reviewer. The CCB generally meets weekly to review CRs. The Emergency Change Control Board (E-CCB) is a smaller group that reviews and approves emergency decisions. For EIS Change Control, this would consist of EIS's DPM IV approvals and for E-CCB, this would consist of EIS DPM IV's and CCHCS CIO and Operations DPM III approvals.

### 5.2.1 CCB Guiding Principles

Sample CCB guiding principles include:

The CCB comprises at least one representative and alternate from each IT functional area and appropriate non-IT functional areas, including line-of-business representatives.

The change specialist and CCB decide whether more or fewer groups are represented.

CCB members, representatives or alternates will communicate to their respective IT functional areas on a timely basis, and provide follow-up activities.

The change manager will schedule regular meetings of the CCB to be attended by the designated representative or alternate from each identified functional area.

The change owner/requestor, implementer and the change coordinator/administrator may present changes at the CCB meeting.

If the owner or a designated substitute does not represent a change that requires representation at a CCB meeting, then the change is postponed, and the change specialist informs the owner.

The CCB or change coordinator can postpone a change, if it is determined that the change does not follow change policy or is logistically unworkable. The change specialist informs the owner.

5.3 The CCB should follow a defined agenda to maintain consistency and transparency and ensure that the necessary matters are covered. Define CRs, Models, Categories and Classifications

Business or IT personnel can initiate a CR. This wide range of potential change initiators and change activities requires consistent and complete guidance regarding documenting a CR. Fundamentally, the change record becomes the source of truth regarding information from the initial documentation CR to the subsequent recording of data as it progresses through the CR life cycle. Therefore, predefine the attributes of a CRCR. The ITCM policy document must describe appropriate definitions and procedures to cover the range of potential CRs.

The formal change request includes a description of the change, the components affected, business needs, risk assessments, resource requirements and approval status.

### 5.3.1 Change Models

The use of a common practice that defines the CR attributes will ensure standardized methods and procedures. Even with ITIL recommendations, names and definitions vary. The identification of these attributes is critical, because it determines the appropriate workflows for dealing with a particular type of CR, such as emergency CRs, which may have specific authorization and documentation requirements:

**Emergency:** A change request to repair a failure or imminent failure. Typically, this CR is associated with a critical priority (i.e., severe impact and urgency) problem that affects production, causes outages or significant degradation in business, or is accompanied by sufficient business justification. In most cases, this request is executed with limited documentation and is outside the standard change schedule time. It should be reviewed later to ensure that latent errors were not introduced to production.

All Emergency CRs must have a thorough justification to why it is necessary to process on an accelerated timeline. In addition, All Emergency CR must be submitted or approved for submission by an EIS Voting member (EIS DPM IV's) and for Agency CRs will also require CCHCS voting members (CIO and Operation DPM IV Manager).

**Standard (Preapproved):** A preapproved change that is low-risk and adheres to an approved, typically well-tested procedure or work instruction. It is relatively common and is the accepted solution for a specific requirement. It should be documented on a master list of approved standard changes.

**Planned:** A change request submitted within policy requirements for documentation, review and lead time

**Unplanned:** A change request not compliant with policy for documentation, review and lead time.

### 5.3.2 Priority

Based on an ITIL definition, this classification identifies the relative importance of a CR. The CR priority status is based on CR classification variables, with input from the change manager. Typically, this assignment accounts for impact and urgency to sequence a CR to address an incident or problem that must be resolved. This prioritization method can also be used to meet business demands, such as the implementation of an enhancement to an application. Typical priority-level descriptions include:

**Low:** A CR is necessary; however, it can wait until the accepted policy release timelines. The problem has minimal impact or the application change enhancement has limited business impact.

**Medium:** The CR addresses a problem of medium-to-low impact. Customer or IT services are not affected. Business risk is low.

**High:** The CR addresses a severe problem that affects production systems and demands immediate attention. The problem has partially disrupted customer or IT service. Business risk is high to medium (for example, slowed business operations).

**Critical:** A CR is justified to address a problem that affects mission-critical production systems and has disrupted customer or IT service. Business risk is high. (For example, there is an immediate financial impact.)

### 5.3.3 Risk Probability

Risk defines the potential disruption of business operations associated with a given change request. A risk is measured by the probability of a threat or the vulnerability of the IT service to that threat. Typical risk definitions are:

**None:** The CR has no significant potential for disruption.

**Low:** The CR may interrupt or delay business operations, with little impact on commitments:

Requires no work outage

Affects only one noncritical application or system

Affects a limited number of clients

Involves changes that are made during nonproduction hours

**Medium:** The CR may interrupt or delay business operations, which affects commitments:

Requires a limited outage

Affects a few applications or one mission-critical application

Requires a business application redesign or enhancement

Affects more than X clients (use impact for guidance)

**High:** The CR may interrupt or delay business operations, resulting in financial impact to the business:

Requires a widespread outage

Affects multiple business-critical applications

Requires a new business application or a major redesign

Affects more than X clients (use impact for guidance)

### 5.3.4 Business Impact

Impact measures the pain caused by a defective IT service. In most cases, variables such as geography, users and so on help identify the scale. The key criteria are the level of business impact and can be obtained from other sources, such as business impact assessments conducted by business continuity or information security. The intent is to identify a relative score for each service to help understand the level of risk. Ideally, the wording below should be more precise.

Typical impact classification definitions are:

**Low:**

Insignificant business impact in terms of losses or brand damage possible

Notification by the change implementer limited to one IT department

**Medium:**

Significant business impact in terms of losses or brand damage possible

Notification by the change implementer required for a few IT and business departments

**High:**

A major disruption of business activities possible across multiple sites

Notification by the change implementer required for multiple IT departments and business sites

### 5.3.5 Additional Categorization and Classification

Accurate information regarding the IT service and CIs enables the CCB to assess the affected and potential collision of a proposed CR. To improve consistency from data integrity and workflow perspectives, this section offers guidance on common IT services, assets and/or CI groups.

**Development:** Application development covers application activity from mainframe to Web applications.

**Infrastructure:** This typically covers network devices and other WAN "plumbing," including:

Data network circuits — WAN and LAN

Data network devices — routers, switches, hubs and firewall components

Voice components — PBXs, phone switches and mail devices

Specialized printers — metal tag, etc.

Plant/site power maintenance/outages

Plant work shutdowns

**Operations:** Server, database and overall production, including:

Servers — Unix, Intel, AS/400, Linux and OS patching/upgrades

Database upgrades — Oracle, Progress Software, Adabas from Software

Data cleanup — dump/reloads, archival, purging, mass data loads or modifications

Mainframes

Storage — arrays, local disks, tape/cartridge devices and firmware upgrades

**Partners:** Service providers, outsourcers or other third-party partners covering outsourced or multi sourced services. (Example would be SOMS HP, CCHCS-Verizon, etc.).

**Security:** Security processes covering security policy improvements, such as authentication

**Service:** IT services, including software as a service platform as a service and outsourced development

**Support:** Service desk

### 5.3.6 Change Submission and Approval Lead Times

This section defines the lead time required for CRs submission. The expectation is that the change implementer will submit changes with the defined lead time to the appropriate reviewing body. These lead times ensure adequate time for the review of a change request and subsequent approval. CDCR EIS and CDCR Agency have a weekly CCB meeting; lead times should ensure sufficient time for CCB members to review the documentation prior to the meeting and determine whether to approve, reject or request additional work.

CRs need to be submitted by close of business (COB = 3:30 pm) every Friday to: Change.Control@cdcr.ca.gov. This will ensure that the CR will be heard at the next available CDCR EIS and Agency Change Control Board Meeting. Failure to do so may cause a delay in obtaining necessary approvals.

Based on the attributes documented in the CR record, these groups define the change's impact on the infrastructure, users or business. These groups measure change complexity, resources required, analysis of risk, impact and priority to determine the appropriate change model to follow. These models are aligned with specific procedure models that detail the steps needed to handle review and authorization:

**Major:** Major changes potentially affect the department or the entire company. They may affect multiple CIs. Multiple IT departments and business sites must be notified.

**Significant:** These changes may affect a group or department and multiple CIs. Notification will be required for a few IT departments and business departments.

**Minor:** These changes affect a few users and CIs (for example, one to 10 desktops or one server). Notify one IT department.

**Standard:** A preapproved change that is low risk and adheres to an approved, typically well-tested procedure or work instruction is relatively common. It's the accepted solution for a specific requirement.

### 5.3.7 Documenting CRs

Documenting a CR enables organizations to manage the process flow and control changes. Also, documentation creates a record that will retain the complete history of a given change. Different types of CRs will require different degrees of data documentation. However, there tends to be a baseline of required data based on type class, category and the service affected.

**Typical baseline CR record data fields include:**

**Change owner and implementer:** as defined in the policy document.

**Class, category, priority, risk and impact:** as defined in the policy document.

**Change type:** as defined in the policy document.

**CIs:** The requesting group should provide a list of items to the remote group for input into the inventory or configuration management database on a regular basis.

**Brief description:** A short description or title that summarizes the change.

**Business justification:** A reason to perform a change, or the negative impact to the business if a change is not performed.

**Change schedule:** Includes targeted implementation.

**Required support resource fields:** This area includes any documentation that is determined to be a requirement for moving forward to the approval stage.

**Back-out plan:** Included within request (specific field) or attached as an external document.

**Installation document:** Document provided detailed steps for installation. Common document provided by application development to production.

**Turnover document:** Document covering all the configuration artifacts turned over from one technical group to another.

**Approver:** Key groups and individuals required to provide approval prior to the implementation.

**Closure:** The requestor closes request. If the person makes the request on behalf of a business unit, then he or she must receive acknowledgment from that unit once the issue is closed. The requestor must also notify the Change Control Manager once the CR has been completed.

### 5.3.8 CR Documentation Principles

All changes have a business justification, documented resource and a defined feasible technical solution.

Unless previously exempted, any change to the IT production environment requires a change request in the change system.

To the extent possible, change implementers should use IT Change Management forms and workflows to ensure consistency during the execution of standard and repetitive changes.

Use established change priorities as guidelines in the decision. The change manager is the neutral arbiter for assignment review. If an agreement cannot be reached with the change manager, then appeal to the next-most-senior level of management.

For specified change types, such as high-risk/high-impact, changes require documented plans for testing, implementation, back-out, notification and verification of success. Operating or support procedures, such as rerun instructions, problem resolution scripts and other information, may also be required, and support staff must be involved.

Emergency changes are usually the result of a problem and may also require a Remedy ticket.

Emergency changes require appropriate prior notification. However, formal approvals may be obtained after the fact. The change manager must conduct a post-implementation review (PIR) for all emergency changes to confirm that there was a legitimate requirement for the use of the emergency change model, and that all changes were documented. Ensure that testing commensurate with the conventional change model is conducted on the emergency changes to identify latent errors.

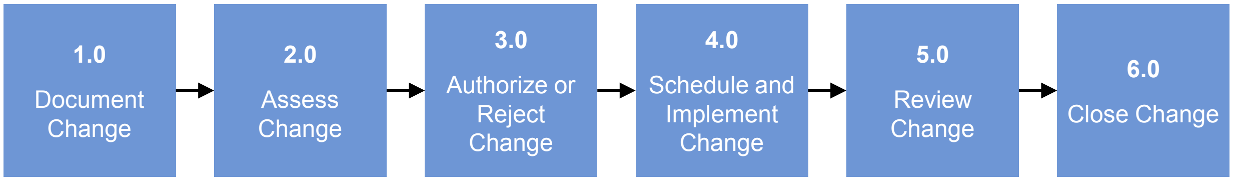
### 5.4 Process and Procedure Workflows

This section offers specific guidance on the ITCM process and procedures. Typical content includes a graphical representation of the workflow, as well as task and procedural descriptions. A good policy guide would cover the macro stage process, procedures, tasks and key integration points with other processes, such as configuration or release management.

The examples below offer basic ITIL workflow content, as well as common procedures and tasks used by midsize to global enterprises. However, we are providing these as examples, rather than recommendations or best practices; they may or may not work for your specific business and production environment requirements.

The change process in Figure 1 presents the common macrosteps or macrostages in the ITCM workflow. This example process flow diagram presents the key tasks needed to be performed to successfully deploy a change. It is consistent with baseline process guidance in ITIL v.3. This graphical workflow is followed by definitional guidance for each stage, mapped to the stage number. Fundamentally, the exercise of defining the various attributes of a change will dictate the established workflow path it follows. The workflow below would be foundational to standard or normal change types.

### 3 Figure 1. Change Management Process



- **Source: Gartner (July 2013)**

**1.0 Document Change:** Submits the CR and provides initial review for validity and completeness.

**2.0 Assess Change:** Reviews the CR categories and presents to the Change Manager and CCB for review and feedback. Assesses the priority and risk of the CR.

**3.0 Authorize or Reject Change:** Presents the CR to the CCB for review, and approves changes based on the CCB recommendations.

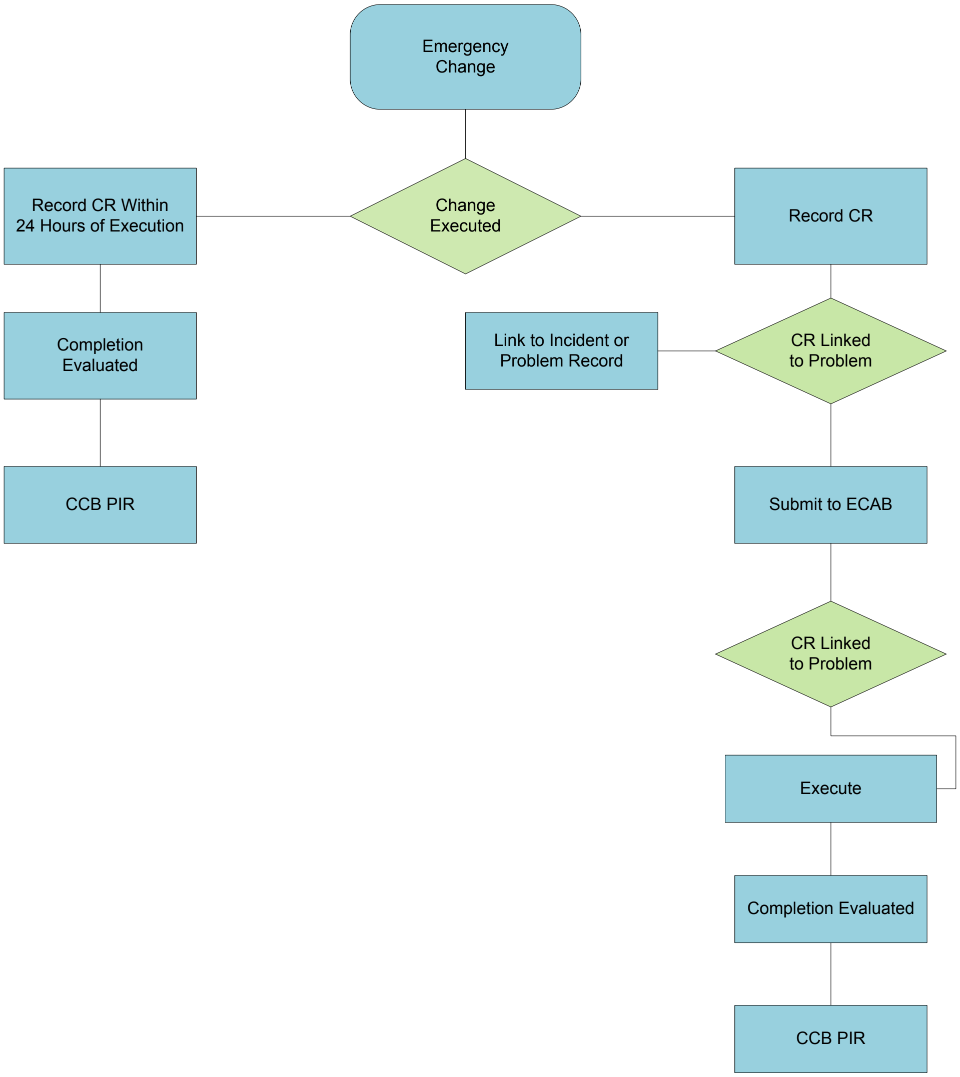
**4.0 Schedule and Implement Change:** Schedules the change and adds to the overall change schedule. Implements the change into the production environment.

**5.0 Review Change:** Reviews the success of the change and determines whether a formal PIR is required. Closes the CR after all subsequent activities and tasks are have been completed. Collects process feedback, than reviews the process for improvement opportunities.

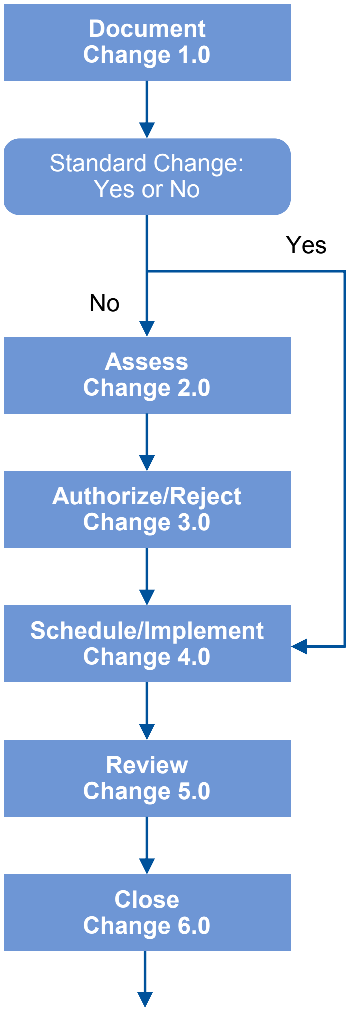
**6.0 Close Change:** The change coordinator will ensure that the CR is properly recorded and documented.

Emergency changes tend to have a separate workflow. In Figure 2, the workflow outlines specific expectations or documentation and approval.

Figure 2. Emergency Change Workflow

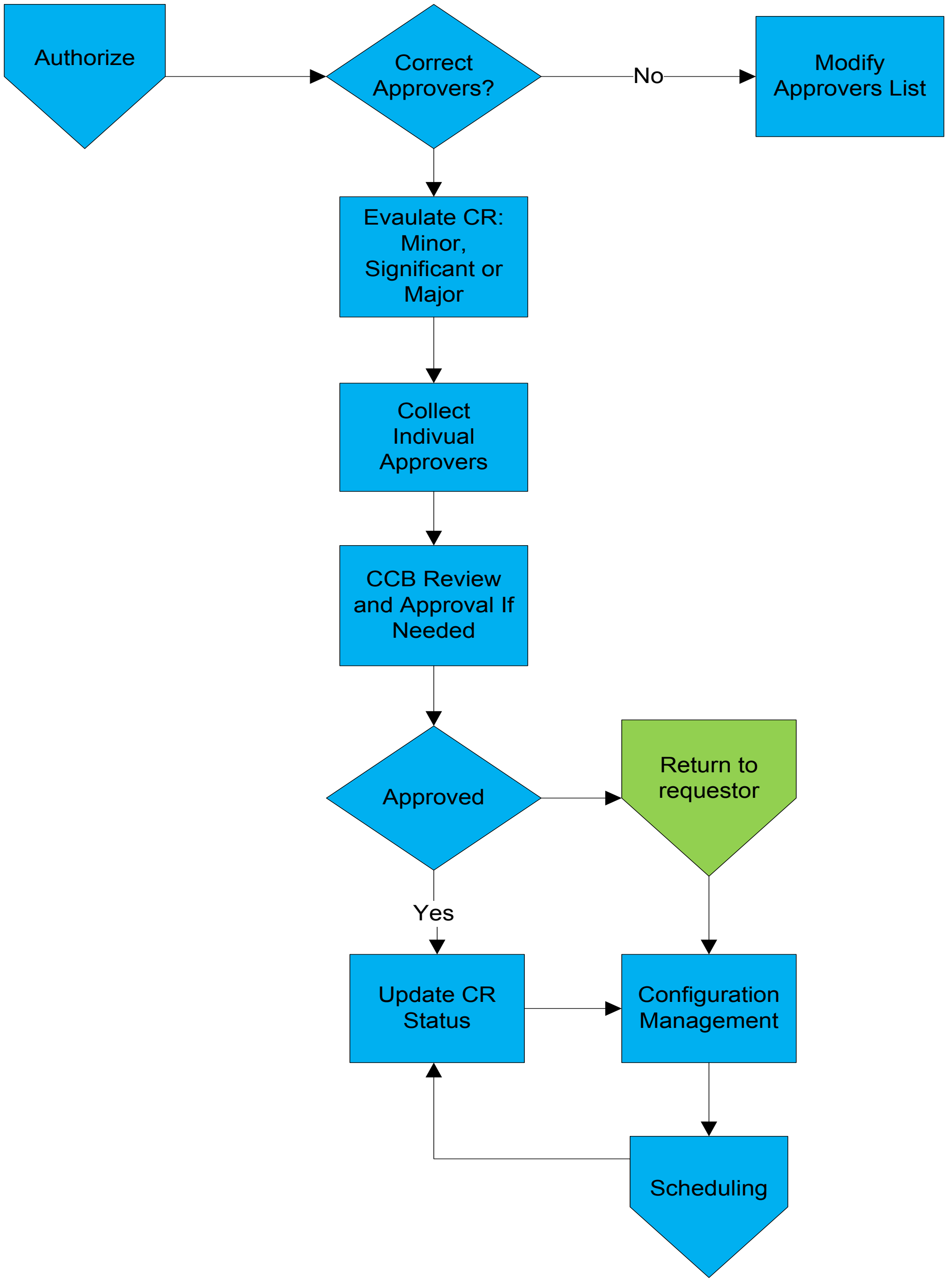


A standard, or "preapproved," change is low-risk and adheres to an approved, typically well-tested procedure or work instruction (see Figure 3). It will also have a modified workflow around the foundational macrostate workflow of change. A well-defined "standard" CR tends to be associated with a preapproved change control workflow. This workflow tends to follow a rule of automatic approval, without needing a CCB vote. This translates into a quick route to the authorization stage. To attain this standard status, the change tasks, procedures and documentation integrity must be reviewed by the appropriate authority. This type of change should be documented on a master list of approved standard changes and on Sharepoint.


Document Change 1.0
Standard Change: Yes or No
Yes
No
Assess Change 2.0
Authorize/Reject Change 3.0
Schedule/Implement Change 4.0
Review Change 5.0
Close Change 6.0

The macrostages may require more microstage activity, such as the task flows assessment or authorization. In Figure 4, this workflow represents an example of established tasks that might be required to complete Stage 2.0 Assess Change, which was presented in Figure 1. Classification and category may require separate approval workflows. Note that the task-level integration with configuration management that acknowledges the update to configuration management is based on the CR approval.

## 4 Figure 3. Change Approval Workflow

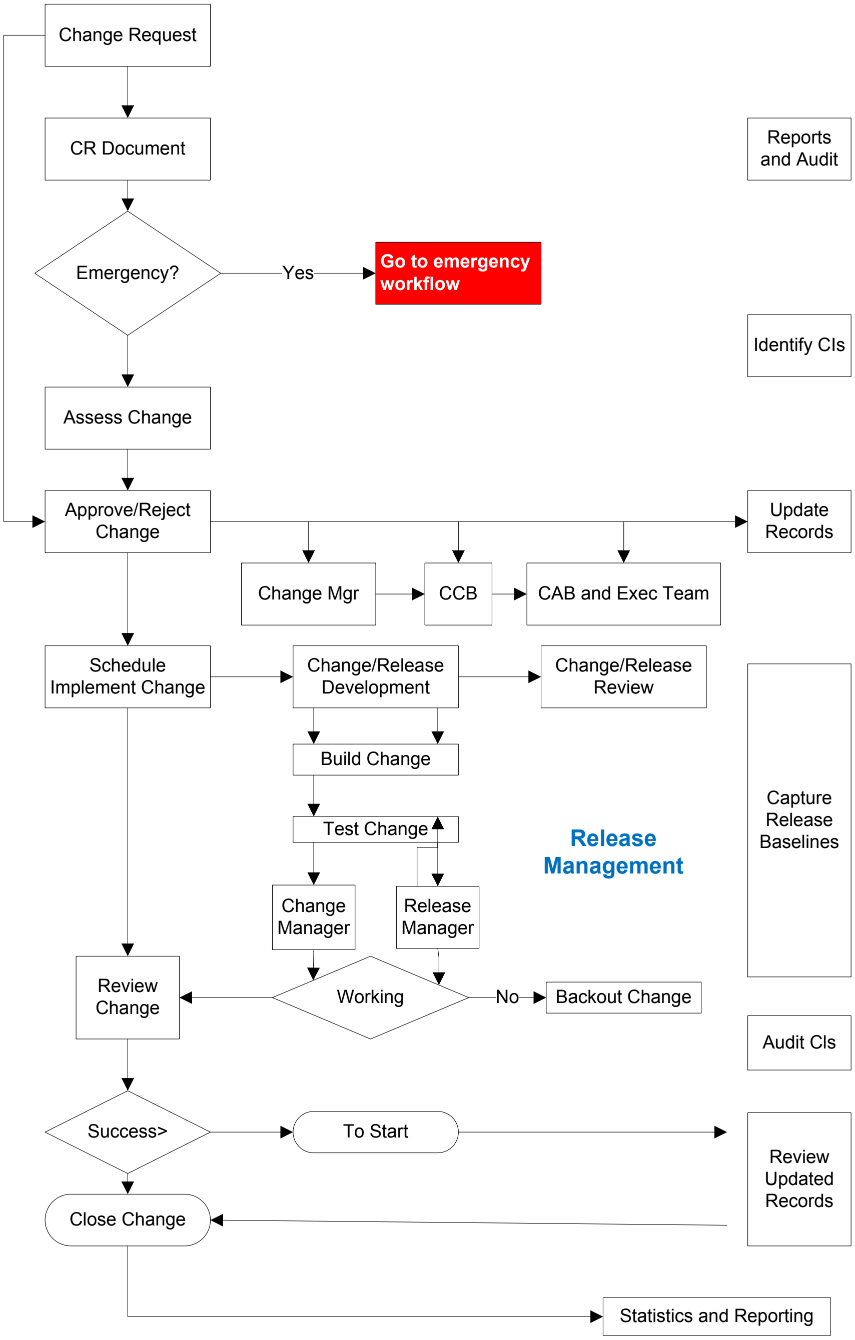


- **Source: Gartner (July 2013)**

Follow the ITCM workflow to synchronize with release and configuration management process workflows. Figure 5 demonstrates key intersection points between configuration and release management with a normal CR workflow. It also includes defined procedure models for the CR categories listed in Section 2.6.5.

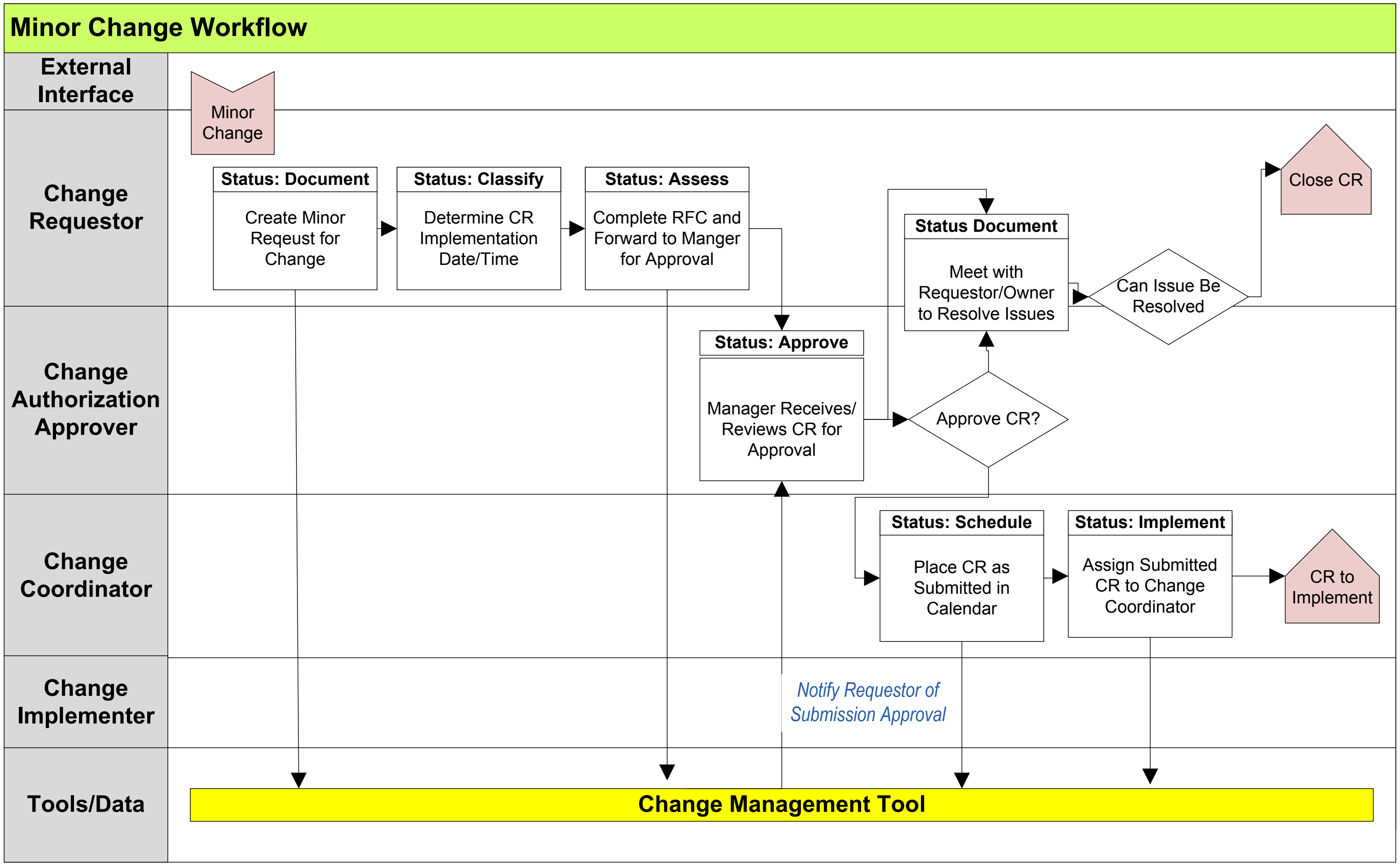
## 5 Figure 4. CR Integrative Process Workflow

Figure 5. CR Integrative Process Workflow



- **Source: Gartner (July 2013)**

6 Figure 5. Change Request Swim Lane


Minor Change Workflow
External Interface
Change Requestor
Change Authorization Approver
Change Coordinator
Change Implementer
Tools/Data
Minor Change
Status: Document
Create Minor Reqeust for Change
Status: Classify
Determine CR Implementation Date/Time
Status: Assess
Complete RFC and Forward to Manger for Approval
Status: Approve
Manager Receives/ Reviews CR for Approval
Approve CR?
Status Document
Meet with Requestor/Owner to Resolve Issues
Can Issue Be Resolved
Close CR
Status: Schedule
Place CR as Submitted in Calendar
Status: Implement
Assign Submitted CR to Change Coordinator
CR to Implement
Notify Requestor of Submission Approval
Change Management Tool

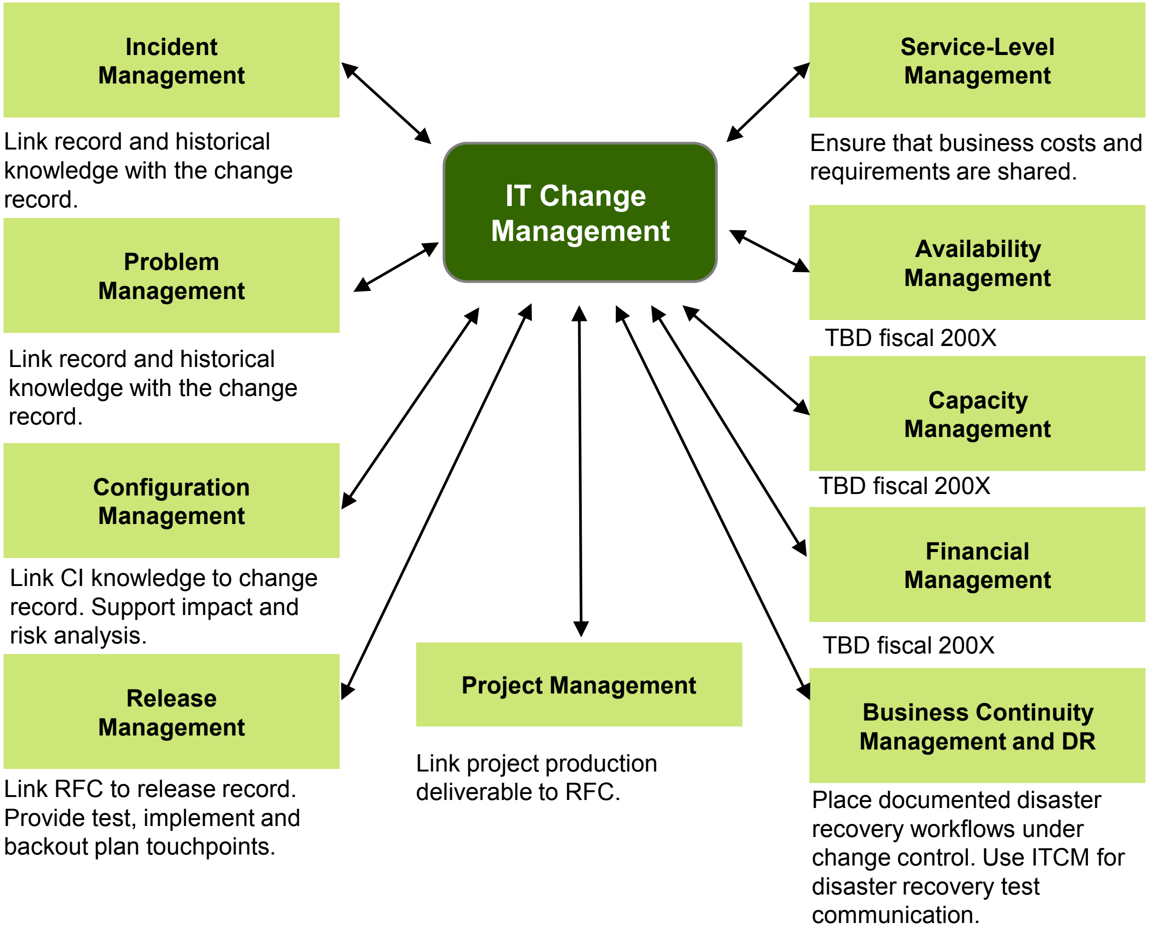
- Source: Gartner (July 2013)

# 6.0 Integrative Process Partners

This section identifies integration exchanges between ITCM and other core IT processes. Although these integration points are critical for long-term ITCM maturity and effectiveness, many of the supporting process partners may vary in degrees of maturity within the IT organization. This small list focuses on a few key processes that may require high levels of integration and ITCM re-engineering efforts as the process integration evolves.

Figure 8 is not exhaustive, and is a typical representation of ITIL-specific process integrations. This can include facilities, manufacturing plant processes, internal audits, third-party vendors and so on. The graphic describes the typical key processes and integration points specific to inputs or outputs to ITCM. (Note: "TBD fiscal 200X" in Figure 7 means "to be determined" in some year.)

7 Figure 6. Linking Key Processes to ITCM


IT Change Management
Incident Management
Link record and historical knowledge with the change record.
Problem Management
Link record and historical knowledge with the change record.
Configuration Management
Link CI knowledge to change record. Support impact and risk analysis.
Release Management
Link RFC to release record. Provide test, implement and backout plan touchpoints.
Project Management
Link project production deliverable to RFC.
Service-Level Management
Ensure that business costs and requirements are shared.
Availability Management
TBD fiscal 200X
Capacity Management
TBD fiscal 200X
Financial Management
TBD fiscal 200X
Business Continuity Management and DR
Place documented disaster recovery workflows under change control. Use ITCM for disaster recovery test communication.

## 6.1 Business Continuity Management and Disaster Recovery

Business continuity management (BCM) maintains and restores mission-critical business processes, personnel and facilities, with the goal of ensuring emergency preparedness and business resiliency. BCM includes six major components:

Risk management and mitigation

Disaster recovery

Business recovery

Business resumption

Contingency planning

Crisis management

Disaster recovery management restores access to production applications and data following a partial or complete interruption of data center operations. It is fundamental to successful BCM, the focus of which is the overall resumption of business operations following the occurrence of one or more disruptive events.

The design of these procedures and plans should be under strict change control to ensure that they are consistent and accurate, and that all stakeholders are aware of the changes. In the case of disaster recovery activity, testing activity can leverage ITCM for communication and may be required to submit a change request.

### 6.2 Configuration Management

Configuration management maintains information about CIs from individual technical domains to IT services. Configuration management should provide guidance on how to collect and federate the wide variety of configuration information into a logical model of service by identifying, controlling, maintaining and verifying the versions of CIs in existence. A configuration management database (CMDB) maintains, federates and reconciles CI data into a single IT service view to support CR analysis. ITCM access to accurate configuration information enables IT staff to assess the impact of proposed changes and to track results.

### 6.3 Incident and Problem Management

Incident management's purpose is to restore normal service operation as quickly as possible and to minimize the adverse impact on business operations, thus ensuring service quality and availability.

Problem management minimizes the adverse business impact of incidents and problems caused by errors within the IT infrastructure, and to prevent the recurrence of incidents related to these errors. Problem management is a key process because changes are often required to implement a fix to a known error. Thus, problem management will generate CR activity and contribute to CCB activity.

### 6.4 Project Management

Project management is a collection of processes focused on the disciplined management of IT projects. The Project Management Body of Knowledge Guide and PRINCE2 offer industry methodologies suitable to manage IT projects covering the organization, control and management of a project. Integration with change management processes will provide analysis and control of identified changes to the IT production environment from project deliverables.

### 6.5 Release Management

Release management coordinates the many sources involved with a significant release of hardware, software, infrastructure and associated documentation across a distributed environment. As part of release planning, identify a release model to correspond with each change model. This upfront planning work reduces ad hoc and error-prone transition approaches

### 6.6 Examples of Key Policy Integration

The release manager must review schedule, track and measure all release events.

The IT change manager and executive CCB must approve and negotiate any changes identified as emergency or off-calendar, or that have missed required lead times.

The release manager must adequately test all changes in the acceptance environments prior to implementation in production. If a test or acceptance environment is not available, then the risk level of the change will be increased appropriately.

# 7.0 Schedule/Calendar

ITCM should coordinate the production and distribution of a change schedule and a projected service impact or availability. A change schedule, formerly referred to as a forward schedule of change in ITIL v.2, contains information about future changes, as well as those that have already been implemented.

## 7.1 Scheduling Key Policy Attributes

Change implementation will take place at predetermined times appropriate to business processes and the functions and cycles they support. All new projects will adhere to these schedules.

Changes must adhere to the approval lead times published in this process guide.

Changes that must be moved from a status of "scheduled" or "in progress" to "postponed" reverts to a status of "requested" and go through the entire CCB review process again.

## 7.2 Change Window Policy

A change window describes the change and release implementation time frame that presents the least impact potential to IT services. Fundamentally, the primary goal of change window policy is to mitigate risks associated with the wide range of CRs proposed on a daily basis. Typically, ITCM policy will define common maintenance windows for change and release activity, such as maintenance, general release and freeze.

The examples below offer maintenance ranges in production fused by a range of midsize to wide enterprises. Therefore, these timelines described in the example window should be seen as examples, rather than recommendations or best practices, as these may or may not work for your specific business and production environment demands.

Maintenance window time frames (see Table 4) typically accommodate standard and normal change types. These changes tend to follow preapproved procedures and tasks, occur on a repetitive basis and have low to no risk associated with them. However, they could require an application or other infrastructure components to be made unavailable for the change to be implemented. Window timelines tend to vary based on production complexity, the size of the application portfolio and business-demand-specific, acceptable planned downtimes.

- **Source: Gartner (July 2013)**

Release windows identify specific time frames (see Table 5) when a release or multiple releases are executed. Typically, the schedule times for releases are documented within the ITCM policy section on scheduling, as well as documented in the release management policy.

- **Source: Gartner (July 2013)**

Freeze windows identify time frames when independent change activity or releases should not be allowed. Typically, these time frames are influenced by business peak activity, high availability and/or regulatory (such as SOX) demands. These windows may be intended to lock down the production environment; however, most organizations find that they can reduce change activity by as much as 95% during the freeze IT organizations that pursue formalized freeze windows achieve high availability during change freezes. This should justify investing in better ITCM policy rigor, so that changes can be made with a lower impact on availability during nonfreeze periods. Common examples of Tier 1 services or mission-critical applications that influence these freeze windows include financial processing, holiday season shopping and student registration. Freeze windows should be documented in the ITCM policy guide change schedule.

### 7.3 Examples of Freeze Windows Policy Content

#### 7.3.1 Month-End Change Freeze

The month-end freeze mitigates operational risks by prohibiting any changes to Tier 1 IT services. (Emergency change requests must adhere to freeze window procedures, as outlined in the emergency change process procedures.) Routine and scheduled changes for these services will be restricted during the last two business days of the month and through the first two business days of the following month.

Nonessential IT-initiated application and system changes will be deferred during this period.

Production rollout for initiatives and projects will not occur during this period.

#### 7.3.2 Quarter-End Change Freeze

The quarter-end freeze mitigates operational risks by prohibiting any changes to Tier 1 IT services. (Emergency change requests must adhere to freeze window procedures, as outlined in the emergency change process procedures.) Routine and scheduled changes for these services will be restricted during the last five business days of the current quarter and through the first two business days of the following quarter. This will overlap with month-end freeze days.

Nonessential IT-initiated application and system changes will be deferred during this period.

Production rollout for initiatives and projects will not occur during this period.

#### 7.3.3 Year-End Change Freeze

The year-end freeze mitigates operational risks by prohibiting any changes to Tier 1 IT services. (Emergency change requests must adhere to freeze window procedures, as outlined in the emergency change process procedures.) Routine and scheduled changes for these services will be restricted during the last 15 business days of the current quarter and through the first 20 business days of the following quarter.

Nonessential IT-initiated application and system changes will be deferred during this period.

Production rollout for initiatives and projects will not occur during this period.

## 8.0 Change Measurement

Measurement and tracking are the keys to constant ITCM process improvement. Measurement and reporting provide management guidance regarding the effect of process performance, identify areas where the process may be ineffectual or broken, and assess improvements overall. The following sections identify measurements that may be used to create various management reports to better understand the effectiveness and efficiency of the execution of the ITCM process.

### 8.1 Critical Success Factors

Based on the strategy and process objectives, the change manager will define, track and report critical success factors:

All changes requests are tracked.

Post-mortem reviews are done consistently and reported.

### 8.2 Quality and Efficiency Metrics

Based on the strategy and process objectives, as well as SLAs and operating-level agreements, the change manager defines, tracks and reports metrics:

Total number of changes processed overall and by change model

Number and percentage of emergency changes

Number and percentage of successful changes

Number of unauthorized changes detected via change reconciliation

Application performance and availability: planned/unplanned downtime associated with changes and the mean time to restore service (MTRS) for Severity Level 1 or Level 2 problems

Ratio of problem- and defect-associated changes

Change volume: looking for month-to-month spikes

Change activity: higher volume or percentage by department, type or item

Change back-outs: higher by department, type or item

Problem/defect: higher by department, type or item

Customer satisfaction with the level of speed and risk management associated with the process

Business impacts of failed changes

Average cycle time for each change model (what lean would term "takt time")

Business value of successfully implemented changes

Number and percentage of failed changes that were approved by the CCB (i.e., the changes were approved, but they still failed)

### 8.3 Compliance and Control

Change management is a key control process, due to its ability to help the organization manage risks. As such, it is routinely audited, and the following tend to be policy attributes that audits may investigate:

Unless a person is classified as an exempted implementer or policy approver, he or she cannot approve or implement changes.

Changes must be submitted in a change management tool by day and time, in compliance with policy lead times, to be considered for review in the weekly CCB meeting.

After implementing a change, the change implementer should set the status to "post review," add any appropriate notes about the implementation to the change request and execute appropriate communication regarding the status of the change.

CR closure requires verification that an approved CR was executed according to documentation. This can be done via various change management roles in concert with auditing or configuration management tools.

The above are examples. If your group is subject to audits, Gartner recommends that you contact internal audit to understand which "key change controls" it will test.

## 9.0 Communications, Coordination and Education Methods

### 9.1 Communications

The ITCM policy must develop and enforce a communication plan that informs IT staff and business stakeholders about the nature and impact of proposed changes. The policy should cover:

Documented policy defining communication scope, purpose, schedule, roles and responsibilities.

Documented communication procedures aligned with CR category and type.

Documented procedures to evaluate and respond to feedback from communication by stakeholders.

## 9.2 Key Meetings

For meetings to be effective, they must occur consistently and follow a defined agenda. All attendees should be aware of the meeting's goals; objectives, expected outcomes and the change manager should track and publish meeting minutes. Attendees should be clear on their roles.

Examples of common meetings include:

Daily change manager reviews

CCB weekly significant and major CR reviews

Problems caused by change weekly reviews

## SOW EXHIBIT-J Advance Pay Options

## SOW EXHIBIT- J PREPAID AND ADVANCEPAY ACCOUNT TRANSACTION FEES DEFINITIONS/INFORMATION

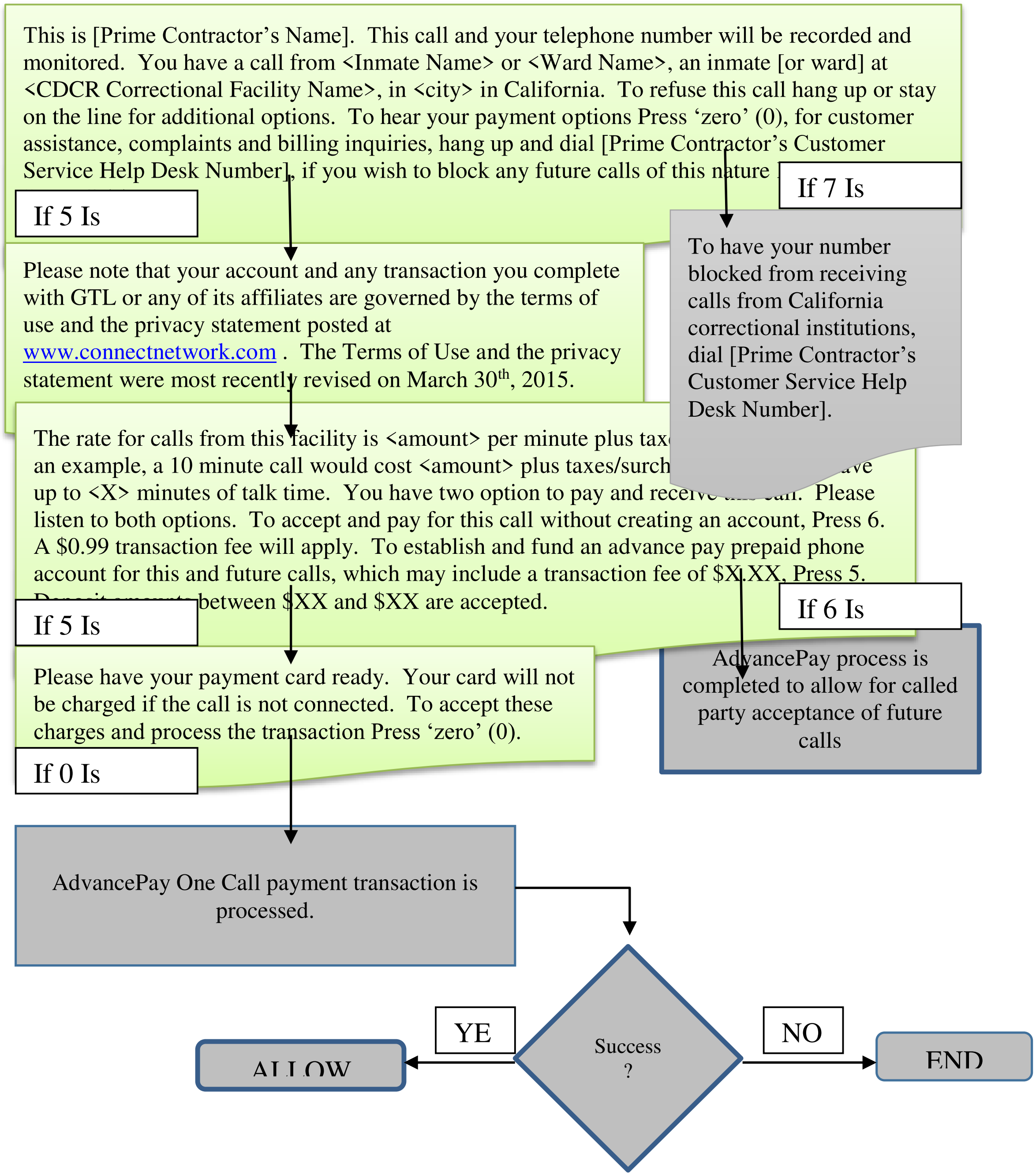
The following information relates to Section 7 of the IWTS/MAS EIS OTP 11-126805, Section 7 Cost Exhibits, as amended, and the PrePaid Account One-time Transaction Fee and AdvancePay One Call Transaction Fee within the Section 7:

### PrePaid Account One-time Transaction Fee

The PrePaid Account One-time Transaction Fee replaces the PrePaid Account Setup Fee to align and be in compliance with the Federal Communications Commission (FCC) new rule § 64.6020(b)(1) For Automated Payment Fees—$3.00 per use. The PrePaid Account Setup Fee was a $4.75 onetime fee to setup a prepaid account. At $3.00, the new PrePaid Account One-time Transaction Fee is significantly less than the onetime setup fee. Although the FCC new rule allows a $3.00 fee to be charged each time automated payment services are used, GTL will apply the $3.00 fee on a onetime basis in keeping with the spirit of the current contract.
This change does not affect prepaid account holders that have already set up an account paying the $4.95 previous fee applicable to the Amendment #3 effective date.

### AdvancePay One Call Transaction Fee

AdvancePay One Call (APOC) is offered by Global Tel*Link Corporation (GTL) to comply with the Federal Communication Commission new rule §64.6100(a), which requires GTL to offer Consumers an option to use Prepaid Calling without a minimum balance requirement. APOC permits the Consumer to use Prepaid Calling at the per-minute-of-use rate for the Prepaid Call at the particular facility. Consumers using an Automated Payment method (§64.6020(b)(1)) to make an APOC will be charged a Transaction Fee of $0.99.
The following diagram is provided only for Illustrative purposes of the call control process that will be used for APOC.



This is [Prime Contractor's Name]. This call and your telephone number will be recorded and monitored. You have a call from <Inmate Name> or <Ward Name>, an inmate [or ward] at <CDCR Correctional Facility Name>, in <city> in California. To refuse this call hang up or stay on the line for additional options. To hear your payment options Press 'zero' (0), for customer assistance, complaints and billing inquiries, hang up and dial [Prime Contractor's Customer Service Help Desk Number], if you wish to block any future calls of this nature

Please note that your account and any transaction you complete with GTL or any of its affiliates are governed by the terms of use and the privacy statement posted at www.connectnetwork.com . The Terms of Use and the privacy statement were most recently revised on March 30th, 2015.

To have your number blocked from receiving calls from California correctional institutions, dial [Prime Contractor's Customer Service Help Desk Number].

The rate for calls from this facility is <amount> per minute plus taxe an example, a 10 minute call would cost <amount> plus taxes/surch ave up to <X> minutes of talk time. You have two option to pay and receive this call. Please listen to both options. To accept and pay for this call without creating an account, Press 6. A $0.99 transaction fee will apply. To establish and fund an advance pay prepaid phone account for this and future calls, which may include a transaction fee of $X.XX, Press 5. Deposit amounts between $XX and $XX are accepted.

Please have your payment card ready. Your card will not be charged if the call is not connected. To accept these charges and process the transaction Press 'zero' (0).

AdvancePay process is completed to allow for called party acceptance of future calls

AdvancePay One Call payment transaction is processed.