



Attachment C

# **Change Control Process**

IT Process

Doc #	07.02.001
Version	.14
Effective Date	May 27, 2016
Reviewed Date:	August 29, 2025

## 1.0 DESCRIPTION

This document describes the process to be followed when making changes to the Tollway's Information Technology (IT) infrastructure and key systems (i.e. Mainframe applications). The Change Control Process is designed to provide a structure in which changes to the IT environment are requested, evaluated and approved prior to their installation or implementation as well as monitored for a brief period after successful implementation. The purpose is to ensure that all elements are in place, all affected parties are notified in advance, and the schedule for implementation is coordinated with all other activities within the organization to ensure that changes are conducted in an efficient manner. In addition, users are requested to review the change and approve that the change addresses their original request.

This process ensures;

- Program changes are approved and authorized by information systems and user management
- Post-implementation reviews are performed
- Procedures exist to ensure that only properly authorized programs are placed in production status
- Program changes are performed by appropriate personnel
- Changes to in-scope systems are documented, tested and approved by Management
- Approved changes migrated to in-scope production systems are performed by personnel authorized to promote changes but without the ability to develop those changes (separation of duties).

## 2.0 SCOPE

The Change Control Process applies to all the types of changes that may be made to the production baseline and is defined as the addition, modification, or removal of an authorized, planned or supported service or service component and its supported documentation.

This process is applicable to any and all changes that are made to software, operating systems, hardware, and the network and can include changes to the IT environment that may arise from many circumstances, such as:

- Problems or incidents
- Periodic maintenance or patches

- User requested enhancements
- Hardware and/or software upgrades
- Acquisition of new hardware and/or software
- Changes or modifications to the infrastructure, including changes to network connections and firewall and router configuration settings
- Operations schedule changes
- Changes in availability
- Changes in response to unforeseen events

The above list is not all-inclusive. Questions as to the applicability of using this process in a particular circumstance should be directed to the Change Control Administrator.

When project delivery affects production environments, the responsibility is on IT management to follow the documented Change Control Processes.

### 3.0 GENERAL INFORMATION

#### 3.1 ACRONYMS

Acronym	Definition
CCA	Change Control Administrator
CRF	Change Request Form
DSS	Data Security Standard
ECAB	Emergency Change Advisory Board
ERP	Enterprise Resource Planning
ISTHA	Illinois State Toll Highway Authority
IRB	Implementation Review Board
IT	Information Technology
ITIL	Information Technology Infrastructure Library
PCI	Payment Card Industry
QMS	Quality Management System
SME	Subject Matter Expert

#### 3.2 DEFINITIONS

Word	Definition
Change	To transform, alter, or modify the operating environment or standard operating procedures; any modification that could have a potential and/or significant impact on the stability and reliability

	of the infrastructure and impacts conducting normal business operations by our customers and IT; any interruption in building environments (i.e., electrical outages) that may cause disruption to the IT infrastructure.
Confidential Information	Information that includes but not limited to the following: Social Security Number, Drivers License Number, Credit/Debit Card Number, Bank Account Number. Reference the Data and Information Classification Policy.
Customer	Person, group or entity that had originally identified the incident or problem and would benefit from the implementation of the change
Emergency Change	During emergent situations there may not be time to follow the normal Change Management process; it is advised to establish an abbreviated process and pre-identify an ECAB to support the process and grant the authorization to perform the change activities.
Event	An occurrence
Incident	Any activity outside of the normal operating procedures that could have a potential and/or significant impact on the stability and reliability of the infrastructure, i.e. a request to keep a system up during a normal shutdown period.
Normal Change	An augmentation to services that is not routine nor an emergency can be classified as a Normal Change. They are planned, tested and verified prior to implementation into production. Other examples of Normal Changes are menu changes, screen changes, updating report changes and database changes.
Immaterial Change	A change to the production environment where the impact of the change is negligible. Examples of an Immaterial Change would be a routine change (i.e. installing a patch), cosmetic changes, reports that only extract information, and non-updating reports.

### 3.3 REFERENCES

	Document Title	Control Number
1	Information Technology Infrastructure Library (ITIL)	v3
2	PCI DSS	Version 4.0
3	Incident Response Plan	07.02.008

4	Document Creation and Change Procedure	07.03.000
5	User Acceptance Form	07.06.006
6	Data and Information Classification Policy	07.01.017

### 3.4 FIGURES

1	Immaterial Change Workflow
2	Normal Change Workflow
3	IRB Review Process

### 3.5 APPENDICES

A	Change Request Form Procedure
B	Emergency Changes
C	Vendor Change Request
D	Change Management Meeting
E	Change Management Priority Designation
F	Change Management Status Designation

## 4.0 RECORDS

Document	Location	Retention Length
Change Request Form	IT Sharepoint	7 years
Change Management Database	IT Sharepoint	7 years
Implementation Review Board Meeting Minutes (to include, but not limited to a list of attendees and the decisions made)	IT Sharepoint	7 years
User Acceptance Form	IT Sharepoint	7 years
Track-It	IT application	7 years

## 5.0 PROCESS

### 5.1 ROLES AND RESPONSIBILITIES

The Implementation Review Board (IRB) is comprised of members representing key functional organizations. They are;

- Chief Information Officer
- Deputy Chief of IT Infrastructure and Development
- Deputy Chief of Operations and Support
- Deputy Chief of OT Ap Development
- Deputy Chief of IT Security

- DBS, SDI Consultant
- Director of OBS Department Electronic Tolling Init
- Chief Operating Officer, Executive Department

The IRB is facilitated by the Change Control Administrator. The Chief Information Officer has the authority to veto any decision.

#### 5.1.1 Originator

The Originator is responsible for;

- Completing the Change Request Form per procedure listed in Appendix A
- In the event of an emergency, following guidelines listed in Appendix B
- As applicable, facilitating Vendor Change Request, as per Appendix C
- Working with the customer to thoroughly understand the problem, developing, testing and implementing the solution, and developing a backout plan
- Clearly defining and documenting the scope of the change
- Documenting the customer impact
- Proposing changes that adhere to applicable policies and procedures
- Performing due diligence prior to implementing change (i.e. testing)
- Addressing all concerns raised by members of the Change Control Board
- Ensuring that the change can be reversed or remedied if unsuccessful and that backout procedures are prepared
- Notifying all potentially affected parties when the change will be implemented, including when the change will be initiated and when the change is completed
- Conforming emergency changes to Change Control Process as soon as practical
- Immediately addressing any compromises to security policies and procedures
- Verifying that the change resolves the original issue

#### 5.1.2 Manager, Originator's organization

The Originator's functional manager is responsible for;

- Ensuring the Originator has sound rationale and justification for proposing the change (i.e. operational, quality, productivity, financial)
- Ensuring the Originator has performed due diligence prior to implementing change

#### 5.1.3 Customer/User

The Customer/User is responsible for;

- Creating a Help Desk ticket and/or completing the change control form

- Working with the originator (and other designated parties) in developing and implementing the change, as applicable
- Validating that the change resolved the incident
- Approving the change as applicable (i.e. signing the User Acceptance form)

#### 5.1.4 Change Control Administrator

The Change Control Administrator is responsible for;

- Ensuring that the Originator properly completes the CRF
- Verifying there is a backout plan
- Coordinating the changes, events and status of the change and that changes are based on priority and risk
- Notifying parties of conflicts needing resolution
- Posting the change schedule that notifies people affected by the change
- Ensuring that non-conformities are recorded and actioned
- Reviewing emergency changes to verify that they were true emergencies
- Ensuring that emergency changes conform to the Change Control Process as soon as practicable
- Facilitating the IRB (per Appendix D), ensuring status of the change is appropriate (Appendix F), and maintaining records as applicable
- Ensuring all votes are accurately recorded for each change
- Escalating concerns to the Chief Information Officer as applicable
- Ensuring that meeting minutes are available to IRB members at the earliest possible convenience. The minutes may include weekly statistics on the number and types of changes

#### 5.1.5 IT Manager

The IT Manager is responsible for;

- Authorizing program changes
- Assigning changes to appropriate personnel
- Authorizing changes for production
- Ensuring post-implementation reviews are performed. Signing User Acceptance Form as applicable

#### 5.1.6 Implementation Review Board Representative

The Implementation Review Board Representative is responsible for;

- Attending the Change Control meetings or notifying IRB members in advance of their inability to attend a meeting
- Reviewing the impact of all changes prior to the scheduled weekly meeting

- If applicable, supporting efforts to identify and define the problem, resolve the problem and implement the change
- Providing additional insight on the impact, urgency, cost, benefits and risk of the change on operations and security.
- Supporting efforts to eliminate or mitigate risks in implementing the change and impact of the change
- Determining if additional security controls are required as a result of the change
- Ensuring the Originator has sound rationale for proposing the change and that the change provides a business benefit (i.e. legal, regulatory, operational)
- Ensuring the Originator has performed due diligence prior to implementation
- Verifying that the change has met its objectives, the customers are happy with the results and there have been no unexpected side effects
- Voting yes or no for all purposed changes or motions
- If applicable, verifying functional operability after change is implemented
- If applicable, ensuring that changes to configurations can be verified during change implementation
- If applicable, help developing, preparing and/or supporting the backout plan
- If applicable, supporting efforts to prevent incident recurrence
- If applicable, ensuring that implementation of the change is scheduled at an optimal time (i.e. minimal impact to operations/productivity)
- If applicable, ensuring that proper notification has been provided to affected users, computer operations personnel, and/or Help Desk personnel before and after the change is implemented

#### 5.1.7 Chief Information Officer

The Chief Information Officer is responsible for;

- Monitoring and enforcing this process within the organization
- Providing the equipment, tools and resources necessary to fulfill the requirements of this process
- Addressing issues as escalated
- Decision making in the event of an impasse
- Reviewing and approving all exceptions and deviations from this process
- Overruling decisions by other IRB members as appropriate

### 5.2 PROCESS ELEMENTS

#### 5.2.1 Suppliers of Input to the Process



Suppliers to the process are:

- Customer/User Requests
- IT Staff who provide resolution to an incident and/or problem
- SMEs to advise the IRB on business impacts, as required

#### 5.2.2 Inputs

Inputs to the process are:

- HW/SW/Firmware solutions
- IT Staff capable of assessing the scope and impact of proposed solutions
- Current Change Schedule of all changes in the production environment
- Testing and validation results or related change efforts
- Completed Change Control form
- Track-IT ticket

## 5.2.3 Process

### 5.2.3.1 Immaterial Change

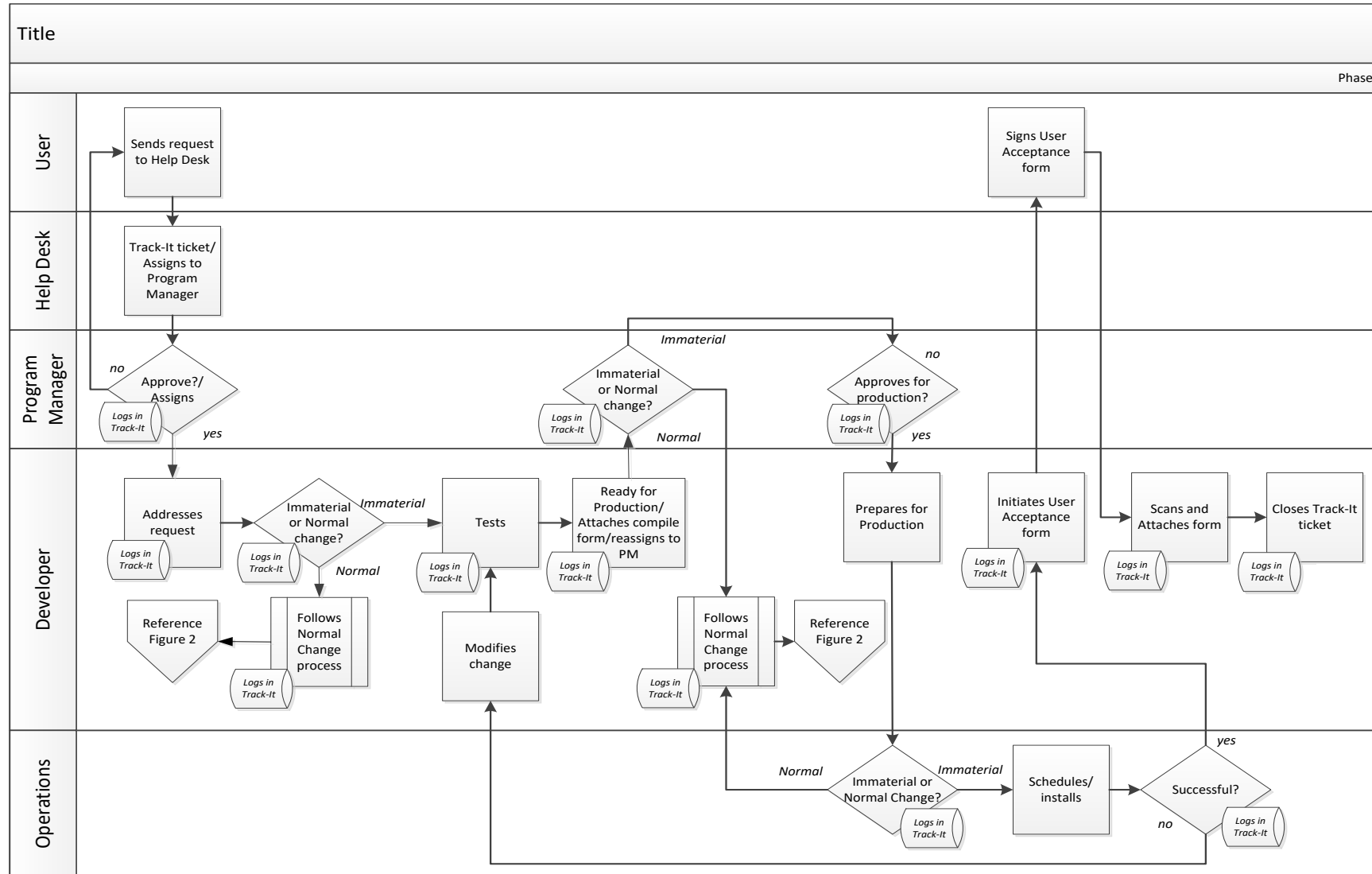
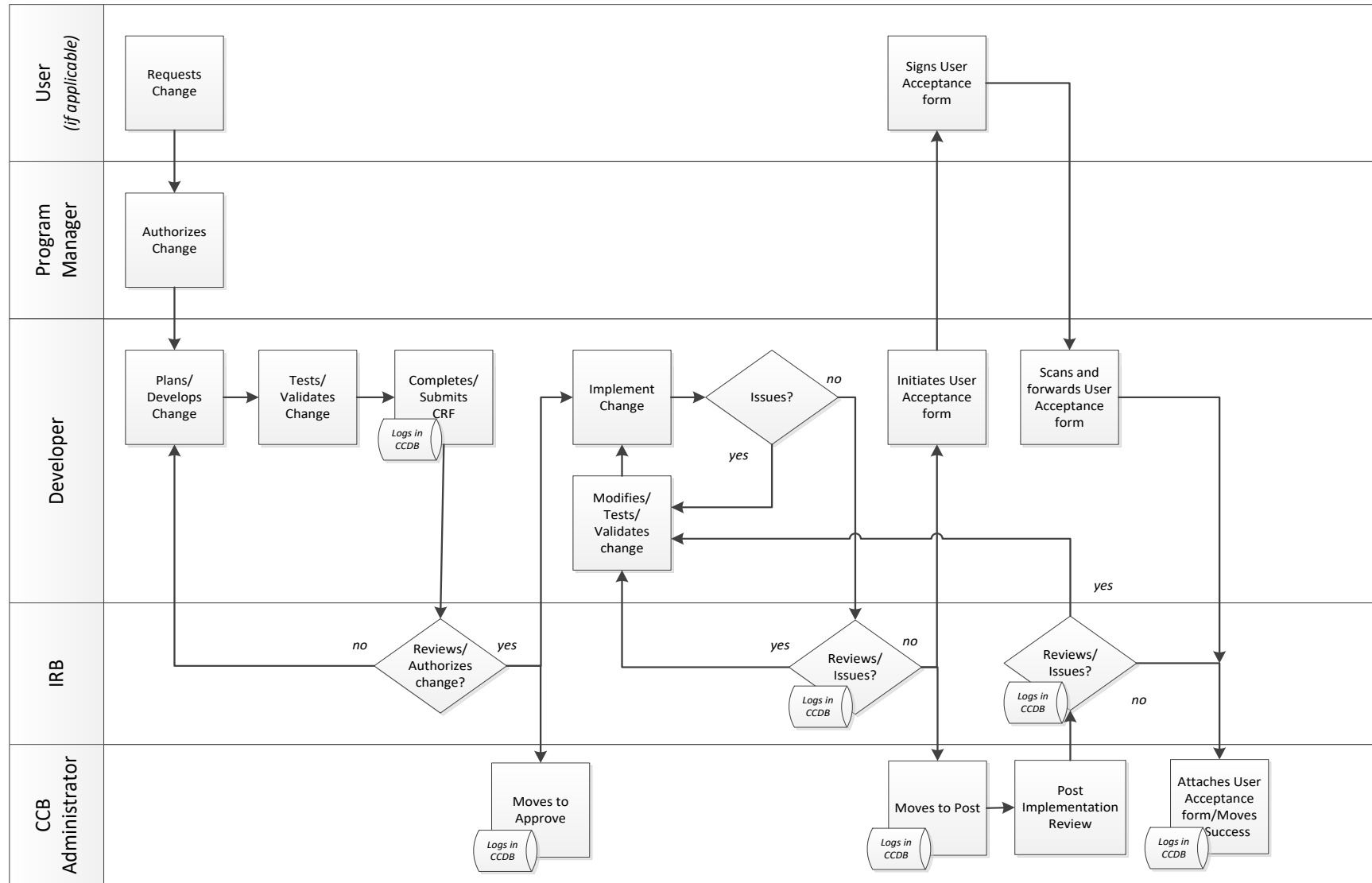
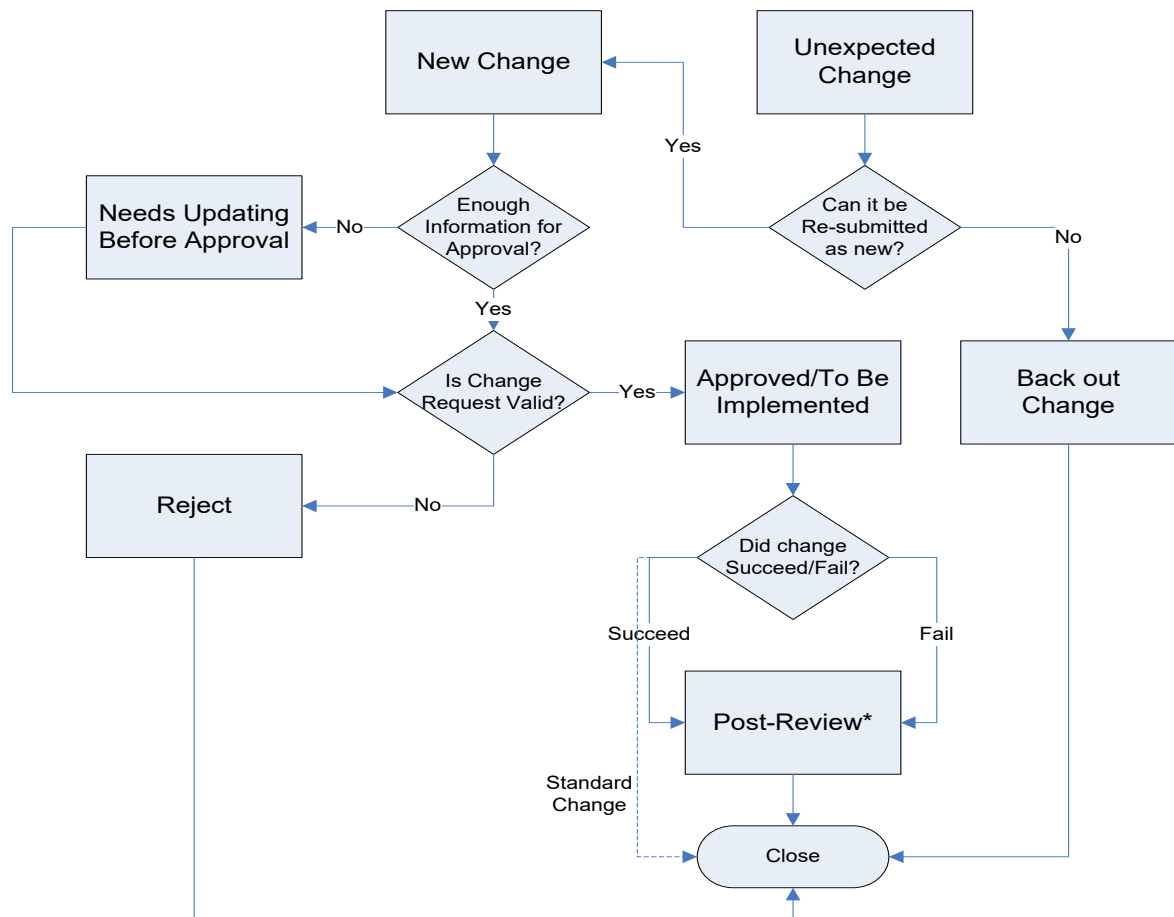


Figure 1: Immaterial Change Workflow

## 5.2.3.2 Normal Change

Figure 2: Normal Change Workflow

#### 5.2.3.4 IRB Review



\*The Post-Review phase includes any testing and documentation that is needed to verify that the change that has been implemented was successful. Not all change control items will need a test plan but in the event that one is needed it will be part of the Post-Review portion of the overall workflow.

*Figure 3: IRB Review Process*

#### 5.2.4 Outputs

Outputs of the process are;

- Solution to resolve the incident and/or problem
- Initiation/Revision to applicable Documentation and/or configuration files have been completed to reflect the change
- Update Change Control database
- Updated Track-It ticket
- Approved User Acceptance Form

### 5.2.5 Customers

Customers of the process are;

- Person who reported the problem
- IT Systems' users who may benefit from the solution
- IT Systems' administrators

### 5.2.6 Measures of Success

Measures of success of the process are;

- Solution resolves the original incident and/or problem
- Customer agrees that the original incident and/or problem has been addressed by the solution
- Solution complies with Tollway & IT policies, processes and procedures
- Solution complies with PCI DSS requirements
- Solution does not compromise or increase security or business risk
- Solution has negligible or positive impact on other IT Systems
- Solution improves productivity, if applicable
- Solution provides a negligible or positive cost benefit
- Solution has a negligible or positive quality impact to overall service
- In the absence of a solution, an increased understanding and documentation of the system

### 5.3 IRB Voting Procedure

Rules governing the voting process are;

- Quorum for Change Management Meetings is three IRB members
- If quorum is not met, new items may not be approved, however status updates on previously approved items may take place
- The Chief Information Officer can supersede quorum requirements
- If there are items that must be approved and there is no quorum, the Change Control Administrator can request email approval from IRB members (email approvals must be attached to the Change Control Item in the Change Management System)
- There will be a vote taken on all Change Control Items

All votes and use of veto powers will be recorded for each Change Control Item in the comments section.

**APPENDIX A****Change Control Form**

To be completed by Originator prior to submittal

- Name
- Creation Date
- TrackIT#,
- Title of the Change
- Item Type (choose one: HW, SW, Communication, NW, Documentation, Environment)
- Description (of the problem and change proposed)
- Type of Change (choose one: Emergency, Normal,)
- Priority of Change (choose one: High, Medium, Low) per Appendix E
- Risk (choose one: High, Medium, Low)
- Reason for the change (choose one: upgrade, bug fix, maintenance, problem fix, performance improvement, emergency)
- Describe Office Location(s) impacted by the change
- Describe Business Unit(s) impacted by the change
- Describe System(s) impacted by the change
- Describe the Customer impact of the change
- In quantifiable terms, describe the Financial Impact of the change
- Describe the backout plan in case there is a problem encountered during implementation of the change
- Describe test approach to verify effectiveness of the change in addressing the original problem
- Enter Planned Date for implementation of the change, to include time and duration

Upon Approval to implement change:

- Functional Organization Representatives indicate their approval (signing User Acceptance Form)

Upon Approval to make the change permanent:

- Functional Organization Representatives indicate their approval
- If applicable, enter name of customer who approved that the change addresses the reason for the change. Attach supporting evidence if applicable (User Acceptance Form).

## **APPENDIX B**

### **Emergency Change Requests**

Emergencies exist only as a result of:

- Immediate or imminent loss of current or future business
- Addressing a legal concern (i.e. noncompliance with Government Regulations)
- Addressing a security concern
- Addressing a safety concern
- A response to a significant degradation in customer service or public confidence/image,
- A response to an emergency business need.

All emergencies, which shall include program moves (i.e. moving a program from development to production in accordance with approved processes and procedures), are handled on an as-required basis with the approval of the Chief Information Officer, Deputy Chief of Business Systems, Deputy Chief of IT Infrastructure and Development, or Deputy Chief of IT Security, and must follow the guidelines below:

1. Send an emergency approved Change Request Form to the Change Control Administrator either before or within 1 business day after the change occurs.
2. The department manager (or his/her designee) will notify the Change Control Administrator and the IT Help Desk of the emergency change. The notification shall include, at a minimum, the following information:
  - Will the change cause an interruption in service?
  - What additional customers will be affected (in the event a change is needed to fix an outage) and who needs to be notified by the Help Desk?
  - What is the possible work around until the problem is resolved?
  - What is the approximate length of the outage?
  - Notification of resolution.
  - Completion of a Help Desk Ticket to accurately describe the outage.

Emergencies after normal business hours, on the weekend or holidays, will be resolved immediately and reported to the Computer Room as this group provides Help Desk after-hours coverage. A Help Desk Ticket will be generated and staff will notify affected customers, as applicable. A completed Change Request Form must be submitted through the regular reporting process on the first business day immediately following when the change was made.

The Change Control Administrator will review all emergency submissions to ensure the change met the criteria for an Emergency Change.

## APPENDIX C

### Vendor Change Requests

Vendors that control portions of the infrastructure will submit change notifications to the designated IT contact. The IT contact is responsible for evaluating and submitting those changes to Change Control on the Change Request Form, following the same procedures as an internal submission. Change requests must be entered at least 48 hours in advance of the next scheduled CCB meeting for the change to be considered.

Out of cycle change request meetings are at the discretion of the Change Control Administrator.

*An example is AT&T, the Tollway's support vendor for NGN. AT&T will send the notification to the Data Communications Division Manager or the Enterprise Information Services Manager. The respective manager will evaluate the request, complete the Change Request Form, and submit the request through the normal process.*



## APPENDIX D

### Change Management Meeting

A weekly Change Control meeting will be facilitated by the Change Control Administrator or designee. The purpose of the meeting is to share information, concerns, comments, etc. in a collaborative environment to eliminate potential disruptions of service to IT customers. The primary objectives to be accomplished at each meeting are as follows:

- Review last changes implemented and discuss any pertinent issues or problems encountered. The CCA will document and follow the change through to completion
- Review proposed changes received since the last meeting
- Identify conflicts and ask for resolution from parties involved
- Establish if customers are affected by the requested change and if procedures are in place for notifying these customers once change is approved
- Review and request resolution from Originators, if the change overlaps and/or conflicts with other requested changes
- Review impact of the change. Each IRB Member will express their approval or denial to proceed with the change (i.e. status change)
- Schedule a time frame to implement a change, while considering application restrictions and upcoming events such as month-end/year-end, holiday, and heavy volume days; that is, any justified business need
- Ensure availability of a back-out or fallback plan
- Ensure support is defined and appropriate staff are available in the event of a back-out to the change or a related problem
- Finalize and approve changes that will occur in the upcoming week
- Review and discuss future changes that have been requested and the impact of those changes

Only change requests submitted within 48 hours of the scheduled Change Management Meeting will be addressed at the meeting. A deviation from this policy is at the discretion of the Change Control Administrator and the IRB.

#### Participants

All branches that have the potential to make changes to any component that could have an impact on the IT infrastructure are required to send a representative to the weekly Change Control meeting. In addition, any individual that has submitted a CRF for that week must attend, or send a designee who has knowledge of the change.

#### Note

***If a representative is not present, the proposed change will not be approved unless prior discussion with a member of the IRB has taken place and been documented. It will be up to the discretion of the CCA to remove a CRF or review the proposal at the following IRB.***

***When the IRB is approving to proceed with a change (i.e. status change), if there is a denial by one or more IRB Member, the change will not proceed until concerns are addressed and/or the Chief Information Officer has used veto power to overrule the decision.***

**APPENDIX E****Change Management Priority Designations**

High Priority	The problem is of an urgent nature and can justify an out-of-cycle change. This priority is used for problems that meet the Priority 1 requirements, except that a work-around exists, or performance degradation for which no temporary work-around is available however delay would not cause adverse mission impact beyond that of inconvenience. These changes must still be controlled, tested and approved prior to implementation on a production system. Change Requests that fall into this category may, at the approval of the Division Manager be implemented immediately.
Medium Priority	Routine Change Requests are judged less operationally important than Priority 2 or the time frame is not critical for implementation. This priority may be used for important software/hardware/network maintenance issues such as version upgrades, utility software, etc. This priority may be used for development activity or new requirements providing that the activity cannot be accomplished with lower priority. These problems are resolved and implemented in the next scheduled change cycle.
Low Priority	This priority is intended primarily for new requirements and for fixing capabilities that are currently operational but are difficult or awkward to use. It applies also to non-standard implementations, and other assorted situations.

**APPENDIX F****Change Management Status Designations**

Aborted	<p>The Originator, Customer, or IRB Member has;</p> <ul style="list-style-type: none"> <li>Reviewed the proposed change,</li> <li>Assessed the change, as appropriate,</li> <li>Estimated that implementation of the change would negatively impact current business operations and security and/or increase risk,</li> <li>Estimated that the proposed change would not resolve the original incident or problem,</li> <li>Estimated that concerns with the proposed solution cannot be resolved and an alternate solution is required, or</li> <li>The original incident or problem does not warrant implementation of a change.</li> </ul> <p>Therefore, the proposed change is aborted.</p> <p>The CCA can also abort a Change Request when there is no action or schedule to address the change (the Originator can re-submit the Change Request if and when it is warranted).</p>
Approved-IMP	<p>Each IRB Member has;</p> <ul style="list-style-type: none"> <li>Reviewed the proposed change,</li> <li>Assessed as appropriate, and</li> <li>Estimated that implementation of the change would not negatively impact current business operations and security or increase risk.</li> </ul> <p>Therefore, the proposed change is approved for implementation.</p>
Post Review	<p>Each IRB Member has;</p> <ul style="list-style-type: none"> <li>Assessed the implementation of the change, and</li> <li>Estimated that the change has not negatively impacted current business operations and security or increased risk.</li> </ul> <p>Therefore, the proposed change is approved for continued assessment for a temporary time frame (no less than 1 week of operation).</p>
Successful	<p>Each IRB Member has;</p> <ul style="list-style-type: none"> <li>Reviewed the proposed change,</li> <li>Assessed as appropriate,</li> <li>Initiation/ revision of applicable documentation and/or configuration files have been completed to reflect the change,</li> <li>Estimated that permanent implementation of the change would not negatively impact current business operations and security or increase risk, and</li> <li>Received customer approval that the change has addressed the reason for the change (signed User Acceptance Form).</li> </ul> <p>Therefore, the proposed change is approved for permanent installation.</p>
Unsuccessful	<p>The Originator, Customer, or IRB Member has;</p> <ul style="list-style-type: none"> <li>Reviewed the proposed change,</li> <li>Assessed the change, as appropriate,</li> </ul>

	<ul style="list-style-type: none"> <li>Estimated that implementation of the change would negatively impact current business operations and security and/or increase risk, or</li> <li>Estimated that concerns with the proposed solution cannot be resolved and an alternate solution is required.</li> </ul> <p>Therefore, the proposed change is unsuccessful</p>
Project	<p>The Originator, or IRB Member has;</p> <ul style="list-style-type: none"> <li>Reviewed the purposed change recognizing that the scope is larger than a single change to a system, or the scope of work to be done will be done over an extended period of time</li> <li>The Originator is responsible for submitting individual Change Management Items to cover the changes and outages of work to be done for a project. Status updates of the individual Change Control Items will be handled normally and once completed the Change Control Project item will be updated to reflect that a phase of the project has been completed.</li> </ul>
Needs Updating before Approval	<p>The IRB Member has;</p> <ul style="list-style-type: none"> <li>Reviewed the purposed Change Control Item and found it to be lacking information to proceed with the Change Control Item</li> <li>Additional requests for information will be documented in the comments section of the Change Control Item</li> <li>Once the additional information has been provided, reviewed and approved by the IRB, the status can be changed to Approved</li> </ul>
Notification	<p>The Originator, IRB Member, or Change Control Administrator has;</p> <ul style="list-style-type: none"> <li>Submitted an item for notification purposes only (example: Springfield is working on the LEADS connection and there will be an outage that is outside of the control of the Tollway)</li> </ul>