CHANGE MANAGEMENT – OPERATIONAL GUIDELINE

Authored	Version	Date	Note
ITD	1.0	07/01/2018	Draft
ITD	1.0	08/01/2018	Final

CHANGE MANAGEMENT – OPERATIONAL GUIDELINE

Objectives: The purpose of this document is to provide operational guidelines to ITD staffs in change management process.

Change Management refers to a formal process for making changes to IT systems. The goal of change management is to control the lifecycle of all changes, increase awareness and understanding of proposed changes across an organization, and ensure that all changes are made in a thoughtful way. This framework enables beneficial changes to be made with minimum disruption to IT services.

Change management generally includes the following steps:

- **Planning**: Plan the change, including the implementation design, schedule, communication plan, test plan, and roll back plan.
- **Evaluation**: Evaluate the change, including determining the risk and impact to service availability.
- **Review**: Review change plan with peers and/or Change Advisory Board (CAB) as appropriate to the change type.
- **Approval**: Obtain approval of change by management or other appropriate change authority as determined by change type.
- **Communication**: Communicate about changes with the appropriate parties (Network Coordinators, Department IT Managers, Service Impact Customers, or Citywide Employees).
- **Implementation**: Implement the change.
- **Documentation**: Document the change and any review and approval information.
- **Post-change review**: Update Status in RFC and Review the change for future improvements.

Scope:

This policy applies to all changes associated with infrastructure service and business systems in production. Modifications made to non-production systems (such as Test/Development environments with no impact on production IT Services) are outside the scope of this guideline.

Roles and Responsibilities:

Team Member: Submit Request for Change (RFC) in SharePoint team site, execute RFC once approved by CAB, validate change was successful, and update RFC once complete.

Product Owners: Review and approve technical plan, roll back plan, risks to service. Responsible for overseeing of change and ensure changes are tested, implemented, and communicated according to City Guideline.

Service / Portfolio Owner: Review and approve schedule, communication plan

Change Advisory Board (CAB): Review/Approve RFC in view of department wide changes.

RFC Category:

RFC Type	Risk Level
Standard: Routine Change, Documented procedure, predictable outcome	Low
Normal: Change followed a vested procedure, tested in test environment.	Medium
Emergency: Change that needs to be done immediate or as soon as possible to ensure security protection and/or service availability to production environment.	High

The risk level given to an RFC will be determined by scale of impact to citywide services in conjunction with risk factor.

Change Definition and Risk			**Risk**		
			3 - Low Issue prevents the user from performing a portion of their duties.	2 - Medium Issue prevents the user from performing critical time sensitive functions	1 - High Service or major portion of a service is unavailable
Impact	3 - Low	• One or two personnel • Degraded Service Levels but still processing within SLA constraints	3 - Low	3 - Low	2 - Medium
	2 - Medium	• Multiple personnel in one physical location • Degraded Service Levels causing service to fall below SLA or able to perform only minimum level of service • It appears cause of incident falls across multiple functional areas	2 - Medium	2 - Medium	1 - High

	1 - High	• All users of a specific service • Personnel from multiple departments are affected • Public facing service is unavailable • Services that are directly impacting public safety	1 - High	1 - High	1 - High

RFC Submittal/Review/Approval Process

1. Team member submit an RFC in change management team site
2. Product Owner review and approve technical plan, roll back plan, risk level
3. Service Owner review and approve schedule, communication plan
4. CAB review, approve RFC

Note: Emergency RFC can be submitted before or after execution for record keeping.

Timeline (Weekly)

1. Team member submit a new RFC by Wednesday
2. Product Owner review and approve by Friday
3. Service Owner review and approve by Monday
4. CAB review and approve on Tuesday.

Note:

1. Any new RFC not following the timeline will not be reviewed by CAB on the weekly CAB meeting.
2. Blackout dates for RFC execution is two business days before and three business days after pay period end.
3. CAB and ITD Executive team can review, approve emergency RFC anytime.

Change Control Board (CCB) Meeting with Department IT Leadership

CCB meeting is once a month, 2nd Thursday from 2:00pm to 3:00pm

Communication Methodology

Communication for scheduled RFC need to be posted to customers and system owners two weeks prior to change execution. Follow up reminder communication one week, and three days prior to execution date. Communication can be done via email and announcement (helpdesk, intranet)

Recipients:

RFC	Network Coordinators	Department IT Managers	ITD Executives	Citywide Employees
Standard	Yes	Yes	Yes	
Normal	Yes	Yes	Yes	
Emergency	Yes	Yes	Yes	Yes

Note: Please send message to ITD Administrative Officer (Claudia Chang) to get approval from CMO before sending citywide employees.

Communication Template:

Standard RFC: Email / Announcement
Dear Network Coordinators, Department IT Managers, ITD Executives

ITD plan to perform a system maintenance on date. This maintenance is to apply Windows security patches to the following systems.

System Name 1,
System Name 2,

Systems will not be available from time to time.

ITD engineer will send out notification as soon as we complete the maintenance. Please notify service impact customers as necessary.

We appreciate your patience during this maintenance.
Please contact ITD at email@sanjoseca.gov or 408-793-xxxx for any questions or concerns.

Thank you,
Sender Name
Information Technology Department

Normal RFC: Text
Dear Network Coordinators, Department IT Managers, ITD Executives,

ITD plan to perform a system upgrade on Altigen Call Center system on date. The purpose of the upgrade is xxxxx. Altigen Call Center system will not be available from time to time.

ITD engineer will send out notification as soon as we complete the upgrade. Please notify service impact customers as necessary.

We appreciate your patience during this system upgrade.
Please contact ITD at email@sanjoseca.gov or 408-793-xxxx for any questions or concerns.

Thank you,
Sender Name
Information Technology Department

Emergency RFC:
Dear City Employees,
ITD Engineer needs to apply an emergency fix to service xxxxx.

Xxx service will not be available for a duration of xx hours, from time to time.

We appreciate your patience during this emergency service.
Please contact ITD at email@sanjoseca.gov or 408-793-xxxx for any questions or concerns.

Thank you,
Sender Name
Information Technology Department

Communication Frequency:

RFC	Target	Reminder 1	Reminder 2
Standard	2 weeks prior to execution	1 week prior to execution	3 business days prior to execution
Normal	2 weeks prior to execution	1 week prior to execution	3 business days prior to execution
Emergency	ASAP	None	None

Completion of RFC

All RFC shall be completed within one month of requested date. Status shall be updated in RFC accordingly.