Change Management Policy

Policy #: TC-ITS-120 **Approved By**: Paul Hopingardner, County Executive, Technology & Operations
Version #: 1.2 **Effective Date**: December 1, 2015

Accountability & Responsibility

This policy is governed by the accountability and responsibility section found here.

Purpose

Change management is one of the most important components to an organization. Implementing a formalized Change Management process enables the organization to more effectively manage change and reduce the risk associated with deploying change. The key components of a Change Management process are

- Approval
- Communication
- Impact analysis
- Mitigation of risk
- Reporting
- Tracking of requests
- Trend analysis

Changes made to non-priority ITS components - such as systems that are not yet in production, development environments or testing environments - are outside the scope of this policy.

Policy

All changes to ITS services must follow a standard process to ensure appropriate planning and execution.

Changes will be categorized as a routine or an emergency change. Appropriate processes and levels of review shall be applied to each type of change commensurate with the potential of the change to disrupt Travis County operations.

It is the responsibility of the Division Director to ensure that all areas under their direction have documented processes that meet minimum standards, are reviewed annually, and are communicated to staff. The Division Director serves as Change Authority by default and is ultimately responsible for ensuring that changes are made in a manner appropriate to their impact on ITS operations.

Minimum Standards

1. All changes must follow a process of planning, evaluation, review, approval, and documentation.
2. All changes must be presented to the Technical Advisory Board (TAB) for input, advice and approval.
3. All changes approved by the TAB will then be presented to the Change Advisory Board (CAB) for input, advice and approval.
4. All changes deemed emergency must be presented to TAB/CAB after the fact for input and discussion.

Policy Revision

Version	Purpose/Changes	Editor	Date
1.0	Policy Creation	Paul Knight Joyce Miller Ryan Reed	12/01/2015
1.1	Updated name of CIO	Randy Lott	12/18/2017
1.2	Updated policy number from 133 to 120 and title of approver	Joyce Miller	11/20/2019

Continuity of Operations Policy

Policy #: TC-ITS-125 **Approved By**: Paul Hopingardner, Chief Information Officer
Version #: 1.5 **Effective Date**: May 30, 2015

Accountability & Responsibility

This policy is governed by the accountability and responsibility section found here.

Purpose

The purpose is to determine criticality of specific applications and data, establish and implement procedures to enable continuation of critical business processes for protection of the security of sensitive information while operating in an emergency mode and provide a process for data recovery.

Policy

The Travis County Chief Information Officer (CIO), or their designee, must identify the levels of emergencies and associated responses. The CIO, or their designee, must develop specific components of the Continuity of Operations Plan, maintain those components, and periodically test the plan. The plan shall be routinely updated and include activities for responding to a system emergency including performing backups, preparing critical facilities, providing authorized access to sensitive information, and providing appropriately detailed migration plans for recovering from a disaster.

Procedures:

Applications and Data Criticality Analysis

Travis County should assess the critical areas of the business, which would include:

- Critical business functions
- Critical infrastructure
- Critical information or records

The specific components of applications and data criticality analysis must include the following:

- Network architecture diagrams and system flowcharts that show current structure, equipment addresses, communication providers, and system interdependencies.
- Identification and analysis of critical business processes surrounding sensitive information.
- Identification and analysis of key applications and systems used to support critical business processes.
- A prioritized list of key applications and systems and their recovery time objectives.
- Documented results of an analysis of the internal and external interfaces with key applications and systems.
- Adequate redundancies within the network infrastructure to reduce or eliminate single points of failure.
- Mitigating controls or work-around procedures in place and tested for single points of failure that are unable to be eliminated.

Continuity of Operations

The CIO, or their designee, must identify the levels of emergencies and associated responses. Travis County will perform annual testing of the Continuity of Operations procedures or an authentic event fulfils the annual testing requirement.

Those levels may be based on the magnitude of the incident or disaster, such as the following:

- *Level One Emergency* may relate to a loss of business function or a specific part of a location/site.
- *Level Two Emergency* may be based on an incident impacting multiple business functions or multiple locations/sites.
- *Level Three Emergency* may be based on a significant disruption to several business functions or substantial damage at one or more locations/sites.

The specific components of a continuity of operations plan must include the following:

- Identification of crisis management team members throughout the organization who will address strategic response of the organization in an emergency.

- Identification of support team members who will address tactical response of the organization in an emergency.
- Identification of a command center or other specifically designated facility to be used during business continuity.
- Identification of sensitive information that would need to be obtained during an emergency.
- Process for acquisition of additional human resources with applicable skill sets if current human resources are geographically restricted.
- Procedures and checklists to provide for the orderly transition and restoration of normal business operations (such as moving from the impacted site to the alternate site).
- Coordination of available critical facilities for alternate processing and business workspace for continuing operations in the event of an emergency.
- Communication plan for internal employees as well as external business partners and other stakeholders that addresses essential issues (such as Human Resources, Business Status, and Financial concerns).
- Procedures to ensure that health and safety issues are addressed.

Policy Revision

Version	Purpose/Changes	Editor	Date
1.0	Travis County Information Technology Services Information Security Policies Creation	Randy Lott	05/30/2015
1.1	Changed title to Continuity of Operations Policy. Merged Applications and Data Criticality Analysis Policy (104) into this policy.	ITS Policy Committee	08/31/2016
1.2	Merged Contingency Operations (202) and Contingency Plan (109) into this policy. Merged Disaster Recovery (111) into this policy. Merged Emergency Access (307) into this policy.	ITS Policy Committee	09/23/2016
1.3	Added annual testing to the procedures.	ITS Policy Committee	09/28/2016
1.4	Updated name of CIO	Randy Lott	12/18/2017
1.5	Updated policy number from 108 to 125 and updated approver's title.	Joyce Miller	11/20/2019