WILLIAMSON COUNTY
1848

Williamson County Technology Services

6.5. Public Safety Software Configuration Policy

DRAFT Version 1.0

Approvals

Policy Approval Date: Date

Final Approval By: Richard Semple, IT Operations Director

Policy Effective Date: Date

Next Review Date: Date

Version Information

This version supersedes all previous versions and all others should be considered obsolete.

Version History

Version	Approved Date	Effective Date
1.0	Date	Date

Scope

This policy applies to all software and hardware that is part of Williamson County's Public Safety Software Suite. A full list of software can be obtained by contacting Technology Services. Generally, however, the following areas are covered by this document:

- Computer-Aided Dispatch software
- Mobile Computer Terminals (MCTs)
- Law Enforcement Records Management Systems (RMS) software
- Fire RMS software
- EMS System Status Management software
- Paging/Toning
- Interfaces
- Two-Factor Authentication
- Mobile routers

Purpose

Provide process and structure for configuration changes to public safety software systems in use at Williamson County.

Definitions

Configuration Change

A configuration change as defined by this policy is: alterations to features and functionality of the software, hardware, or processes that impact any agency or the support & maintenance of the system.

A configuration change is NOT:

1. Edits to users/personnel (new, deletes, rights changes)
2. Edits to units (adds, deletes, capability changes) within defined unit types
3. Internal departmental workflow, process changes
4. New projects (new hardware, software, or major process implementation)

Departmental Configuration Changes

Configuration changes that are determined to only affect the submitting department are Departmental Changes and do NOT go to the Governing Body. These are evaluated and implemented by the Department and/or Technology Services directly.

Emergency Configuration Change

Configuration changes that occur, and are relevant to, one of the following conditions is considered an emergency configuration change:

- Loss of essential functionality due to unplanned hardware or software changes or failures
- Natural disasters or other declared emergencies that change business practices
- Personnel changes that are unforeseen and have an immediate and major impact to operations
- Other situations that are approved by the Manager of the Public Safety Technology Division of Technology Services

Governing Body

The group or team of department representatives that has been charged with the general oversight of the software, hardware or process. The Governing Body is an information sharing and advisory group that helps set the direction for use, standards, future development, and prioritization of issues. Technology Services manages the software and hardware on behalf of the customers and the Governing Bodies.

These are currently defined as:

CAD/MCT	**Dispatch Steering Committee**
CAD Interfaces/related software	**Dispatch Steering Committee**
Deccan	**Dispatch Steering Committee**
Fire RMS	**Dispatch Steering Committee**
Law RMS/MFR	**RMS Team**

Multi-Agency Configuration Changes

Configuration changes that impact more than one agency are considered “multi-agency” configuration changes that require the approval of the appropriate body before completing the Configuration Management workflow.

Policy

Initiating Configuration Changes

The department head or designated agency Point-of-Contact should submit a Change Request Form found on the Technology Services SharePoint Page. This form is an important first step to capture the basic information so that more conversations and discovery can take place.

Configuration Management

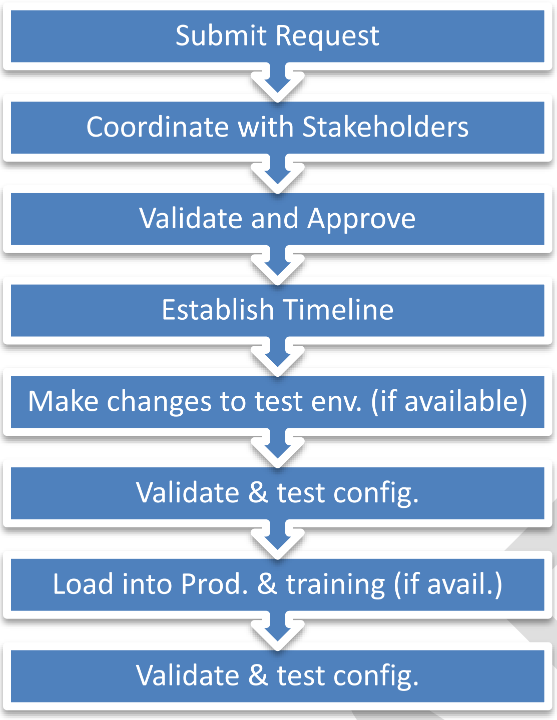
If the configuration change requested falls under the definition of a Departmental Configuration Change, the timeline and test plan will be mutually developed by Technology Services and the submitting department. Many times, the scheduling will be determined by the location in the queue, priority, severity and external deadlines.

Multi-Agency configuration changes will be routed to the appropriate Governing Body for consent after an initial review. When the Governing Body consents (or has delegated consent), then the timeline and test plan will be developed.

If the configuration change requires contracts or large changes to the scope of the project, additional approvals may be required. For example, work contracted out may require a Scope of Work and contract from a vendor, which means that the County Commissioner’s Court may need to consent to the work.

Whenever possible, changes will be first loaded into a test environment and run through a series of test scripts to validate the configuration. After this the production (live) environment and any applicable training environments can be updated. A final validation will take place after loading into the live environment.

These changes will follow this general workflow:


Submit Request
Coordinate with Stakeholders
Validate and Approve
Establish Timeline
Make changes to test env. (if available)
Validate & test config.
Load into Prod. & training (if avail.)
Validate & test config.

Delays or Rejections of Configuration Changes

Changes can be rejected or delayed at any step in the process for several reasons, however the intent of the Configuration Management process is to enable change, not reject it. Some reasons for delays or rejections may be:

- Outside Scope – The configuration requested changes the defined scope of the project, the support model, or other parameter that would modify the project beyond the intended scope.
- Large Impact – The configuration requested would create a burden on another agency (for workload, support, etc.) that is not able to be sustained in the current form.
- Violation of policies or laws – configurations that would run contraindicatory to County policy, local, State, or Federal law
- Funding – sufficient funding is not in place to support the requested configuration at the current time.
- Other reasons as justified by the Technology Services or the Governing Body.

In the event of rejection, it is incumbent on all parties to come up with alternatives that are suitable to the department requesting the change while satisfying the concerns of stakeholders.

Emergency Configuration Changes

Certain unforeseeable circumstances require modification to configurations to be made with little to no time to test and validate the change. These are exceedingly rare, but even in a verifiable Emergency, the change will still go through the Technology Services Change Management process. However, the change may be made in advance of the approvals and testing at the discretion of the Public Safety Technology Manager (or superior) and the change will route through the process after for review and final approvals.

Special Note: Agency Map Area Changes

Configuration Changes Due to Annexations

Configuration modifications to response boundaries due to the annexation of a city are generally updated by the Public Safety Technology staff after notice from the city. However, if the city has not notified the GIS or 9-1-1 Addressing groups, the department may initiate the change by contacting the city as well as the Public Safety Technology staff.

Configuration Changes based on Agreements/Contracts

All changes to agency map layers must be approved by the Chief or designated Point-of-Contact (POC) in writing. A map showing the proposed change is required. A paper map or digital file may be submitted illustrating the changes to be made.

As all boundaries of the agency layer touch another agency, each change means that at least two department's areas will be affected. Therefore, all changes to this layer must be approved by all of the affected departments.

This approval must come from each affected Chief or a designated Point-of-Contact (POC) in writing. One map showing the change needs to be signed by each Chief or POC and submitted to the Public Safety Technology Division. Alternatively, if a written agreement between departments or between an ESD/City and a fire department exists already, that document can be submitted to the Public Safety Technology Division.

If additional map or technical support is needed, as well as when the configuration change requests are ready to be submitted, a work order must be sent to Williamson County Technology Services Staff.

Exceptions

The Manager of Public Safety Technology (or superior) may exempt specific configuration requests from this process on a case-by-case basis, however, this must be used sparingly and full justification and documentation of such exemption must be made under the Technology Services Policy Exemption form.

Policy Violations

A violation of this policy might result in violations to other County policies, state or federal law. Violations of applicable laws may incur legal consequences, and violations of County policies may lead to loss of access to particular resources, and/or disciplinary action up to, and including, termination. All violations will be referred to the department head or elected official and any other appropriate County officials.