



BOBBY JINDAL
GOVERNOR

State of Louisiana
Governor's Office of Homeland Security
and
Emergency Preparedness

MARK A. COOPER
DIRECTOR

Information Technology Change Management Policy
Policy Number: GEN-0015

Issue Date: August 6, 2010

Effective Date: August 6, 2010

Revised Date: 12/28/09, 8/6/10

Approval:

A blue ink signature of Mark A. Cooper, written over a horizontal line.

Mark A. Cooper, Director

I. POLICY

It shall be the policy of the Governor's Office of Homeland Security and Emergency Preparedness (GOHSEP) that the agency's Information Technology Section shall establish and maintain the Policies and Procedures for all application and database change management systems within the GOHSEP.

II. PURPOSE

- A. Develop and maintain clear, concise, and consistent policies and procedures across the GOHSEP distributed systems enterprise.
- B. Establish a formal process of making changes or granting access to make changes to the various applications and databases maintained and supported by the GOHSEP Information Technology Section or by contracted third party developers / vendors. Changes to applications and or databases will be scheduled in advance to allow for development, analysis and testing of changes on an as needed basis or in emergency situations when necessary.
- C. The Information Technology Section is responsible for facilitating the change management process and applying Industry Best Practices when applicable.

III. APPLICABILITY

This policy applies to all GOHSEP Systems, Application and Database Administrators' and Third Party Administrators working for GOHSEP.

IV. PROCEDURES

- A. All requests for changes to the IT environment and or a hosted application / database must be made using the Track-it work order system. Once the change request is submitted into Track-it; a *change coordinator* will be assigned based on the application / database owner and an approval chain will be established based the application / database owner and the affected sections. The Track-it work order must include the following information:
1. Contact Information: The requestor's name, position, and contact information.
 2. Description: A description of the change, including the nature of the change and a description of the item(s) to be changed.
 3. Reason: The reason for the change, including a cost-benefit analysis and any budgetary approvals required.
 4. Priority: A suggestion of the priority and category of the change based on the information currently available. The following priorities are to be used:
 - a. Emergency – A change that will cause significant damage or risk of damage to GOHSEP if not implemented immediately, such as major security patches.
 - b. High – A change that is important and should be implemented soon, such as software changes required to meet reporting and or regulatory requirements.
 - c. Medium – A change that provides benefits to GOHSEP such as an enhancement to a financial planning system.
 - d. Low – A change that is “nice to have” but not needed immediately and has a low impact.
 5. Category: A suggestion of the category of the change based on the information currently available. The following categories are to be used
 - a. Major – The change affects a large part of GOHSEP, such as a section or division.
 - b. Significant – The change effects a smaller portion of GOHSEP, such as a branch within a section.
 - c. Minor – The change effects a small number of users.
 6. Impact: Implications of not making the requested change, to include functionality and/or financial. Include any impact on internal or external service level agreements (SLAs).

- B. Assess the change: The Change Coordinator assesses the urgency and impact of the change on GOHSEP as a whole, considering the scope of the change and its impact on user productivity. This should include:
1. Impact of the change, including how users and GOHSEP will be affected.
 2. Risks involved in making the change.
 3. Risks of not making the change.
 4. Suggested implementation plan.
 5. Describe the change backout plan.
 6. Impact of the change on Continuity of Operations Plan (COOP) activities.
- C. Plan for the change: This includes documenting the steps required to make the change, taking into account the technical requirements of the change. The plan should be optimized to minimize the impact on the IT infrastructure. For major changes the implementation plan should be reviewed by the affected section's management team. The plan must also include steps required to back out or reverse the effects of the change if the change does not have the desired effect.
- D. Approve the change: For all changes, approval or rejection is granted by the assigned approval chain. The approval chain will vary but at a minimum consist of the following:
- a. Application Administrator (typically the requestor/software owner)
 - b. Section Chief(s) (Impacted user community)
 - c. Systems Administrator (Responsible IT staffer)
 - d. Deputy Director (Divisional owner – situational awareness)
 - e. Information Technology Section Chief
- E. Implement the change: Implement the change following exactly the steps outlined in the implementation plan.
- F. Document the results: A review must be made to determine if the change had the desired effect on the IT infrastructure or system changed. Document what went well and what did not; this will help in planning future changes.

V. RESPONSIBILITY

A. Information Technology

- Lotus Notes
- Virtual Louisiana

B. Operations

- WebEOC

C. Information Systems

- Louisiana Public Assistance (LAPA)
- Louisiana Hazard Mitigation (LAHM)

VI. Exceptions

Requests for exceptions to this policy must be submitted to the appointing authority along with specific and compelling justification. Exceptions will be considered and granted when the GOHSEP is operating under a state or federally declared disaster or an elevated activation level and time does not permit for the standard change management process.

VII. Questions

Questions regarding this policy should be directed to the Information Technology Section.

VIII. VIOLATIONS

Employees found to have violated this policy may be subject to disciplinary action up to and including termination.

IX. Appendix

Change Management Work Flow

X. Related Policies

Software Testing Policy

Patch Management Policy

Appendix

Change Management Work Flow

Process

The Change Management work flow process is illustrated in the diagram below. Emergency changes are not reflected in the diagram.

