Policy ID: OIT-23-03.3
Title: Change Management Policy and Procedures
Affected Agencies: Office of Information Technology with outcomes impacting All County Agencies and Departments
Facilitating Department: Office of Information Technology

Chief Information Officer signature:
Date signed and effective: 8/18/2023

1. Overview

The Office of Information Technology has adopted an Information Technology Service Management (ITSM) approach that focuses on implementing and managing IT services that meet the needs of Galveston County. In order to implement and effectively manage service delivery, an ITSM utilizes the Information Technology Infrastructure Library (ITIL) framework. Changes are events that impact production systems. The Change Management process ensures standardized methods and procedures are used for efficient and prompt handling of all changes.

Change Management will work in coordination with Problem, Service Request, and Incident Management to ensure that changes are handled in the best way possible.

2. Purpose

The purpose of this policy is to define standards, procedures, and restrictions for the implementation and management of the ITSM Change Management approach for Galveston County.

3. Scope

All changes which may impact production systems fall under the purview of this policy. Changes are not authorized for implementation unless they follow the Change Management process. Change details and any supporting documentation must be logged and tracked within the County's ITSM software platform, ServiceDesk Plus.

4. Policy

All Galveston County Office of Information Technology staff will enter and document all changes which may or which will definitively impact production systems. Staff will follow the procedures contained within this document to create, follow, implement, test and close changes.

A request for change (RFC) can occur due to:

- An incident that after further investigation necessitates a change is required to resolve the incident. The incident within ServiceDesk Plus drives the change being submitted.
- A problem that after further investigation necessitates a change is required to resolve the problem. The problem within ServiceDesk Plus drives the change being submitted.
- An internal or external employee or a vendor requests production changes. If the request is from an external employee or vendor, the incident or service request within ServiceDesk Plus drives the change being submitted.

Except in the case of an emergency, changes must be approved by the CAB a minimum of 48 hours prior to their implementation. The preferable window of time is five business days. When planning a change, all personnel involved in the change must take into consideration the time required to plan and document the change itself, plus allow for review time by the CAB. Changes will be discussed and/or introduced at a weekly meeting with the OIT management team.

5. Procedures

5.1 Lifecycle of a Change

1. Submission – Change Requester or Change Owner submits a Request for Change (RFC) as a new change within ServiceDesk Plus. This change is driven by an incident request, service request, problem, or internal to OIT. This stage moves from Requested to Planning, Planning in Progress.

2. Planning – Change Owner creates the plan for implementation and backout if needed. At this stage, the Change Owner can Reject or Approve the plan to move on to the CAB Evaluation.
3. CAB Evaluation – The Change Manager reviews the change for accuracy and scheduling. Once approved by the Change Manager, the subsequent CAB members review the change and either Approves or Rejects. If Rejected, the change returns for more information in the Planning stage where it can be canceled or more information can be entered and resubmitted for CAB Approval. If Approved, the change moves on to the Implementation stage.
4. Implementation – Once approved by CAB, the Implementation of the change can take place. The change owner and other members of the implementation team step through the planning process in order to put the change into place. If successful, the change moves on to System Testing. If a failure occurs, the Back Out process is started.
5. System Testing – The change is tested by OIT and the impacted customers. Once completed, the change moves on to final Review.
6. Review – Review of the outcomes and any applicable information for lessons learned are entered.
7. Close – Change is completed and closed.

5.2 Request for Change (RFC)

5.2.1 Step 1 Submission

Any OIT staff member can enter a change on their own or on behalf of an external customer, including a vendor. All changes need to be recorded in ServiceDesk Plus.

Every change that is entered must be evaluated. The "ITIL Seven Rs" are a good starting point when evaluating a request for change:

- Who **raised** the change?
  - This person is valuable because they are the ones with the information to support the change.
- What is the **reason** for the change?
  - Some common reasons may be for capacity, availability increase, or to minimize risk. Be sure the reason aligns with OIT strategy.
- What is the **return** required from the change?
  - Understand what the outcome of the change is going to be. Make sure the return you are getting is sufficient enough to perform the change in the first place.
- What are the **risks** involved in the change?
  - Every change involves risks. However, question how much risk you are going to allow to make sure the change can be administered with that risk present. A regression strategy is necessary if the worst-case scenario does indeed occur.
- What **resources** are required to deliver the change?
  - Make sure you know all the resources you need for the change including money, time, people, equipment and software and that they are sufficiently available to you.
- Who is **responsible** for the build, test and implementation of the change?
  - Ensure you know who is responsible for those three functions and that they separated as appropriate. This is particularly important for compliance and auditing.
- What is the **relationship** between this change and other changes?
  - There are frequently multiple changes occurring at once. Be sure there are no conflicts with other changes at the same time.

Submission details are entered into the change, including defining who is in what role. See Roles and Responsibilities for definitions. Other information is beneficial such as priority, impact and urgency. It helps begin defining who and how the change will affect. The details such as Scheduled Start and Scheduled End should include the implementation phase and beyond – implementation, testing, review and closure.

The Change Owner moves to the next stage, Planning.

5.2.2 Step 2 Planning

The information contained in Planning is the heart of who and what is impacted, how you plan to roll out the change, what happens if something goes wrong, and a checklist of steps to walk through for the life of the plan. All of these fields should be completed as part of this stage.

- Impact details: information about location of the change and who may or will be definitively be impacted by its outcome.
- Rollout plan: describe how you will get your change successfully applied to production and working as expected.
- Backout plan: the steps that will be taken to undo any changes that have been made, in most cases, returning to previous state
- Checklist: a list of tasks that need to be completed prior to or as part of the change. The Change Owner should ensure that all of OIT is informed via email of changes prior to their implementation.
- Schedule: Downtime Schedule should be added for the timeframe where changes that impact production will occur. Freeze windows should be avoided and changes should generally occur within the given maintenance window.
- Associations: If an incident, service request or problem is responsible for the initiation of the change, those item(s) should be selected and associated. This helps in keeping history of changes should a need to retract footsteps occur.

The Planning stage is then sent for CAB Evaluation.

5.2.3 Step 3 CAB Evaluation

Every change must be reviewed by the Change Manager for accuracy, completeness and to ensure it meets the Seven Rs prior to being evaluated by the CAB.

Depending on the priority of the change, the change may go through different approvals.

- **Low** – requires approval only by the Change Manager
- **Normal** – requires approval by the Change Manager and Deputy CAB
- **Medium** – requires approval by the Change Manager and Deputy CAB or Executive CAB
- **High** – requires approval by the Change Manager, Deputy CAB and Executive CAB

The Change Manager and the CAB members have the authority to approve or deny the change. If approved, the change moves to the Implementation stage. If denied, the change returns to the planning stage for further evaluation or cancellation.

The goal of the CAB approval is not to reject or postpone the proposed changes, but to mitigate the risks associated with a poor or lack of business review process, inadequate testing and remediation, implementation, communication and back out procedures.

5.2.4 Step 4 Implementation

The Change Owner is responsible to ensure the change is completed within the change window, ensures all assigned tasks are completed within the change window, and is responsible to make sure the approved change does not get altered after approval and prior to implementation.

Changes that require a deviation to the approved plan need to be immediately halted and escalation procedures enacted. A decision needs to occur between the Change Owner and the Change Manager to either invoke the back out process, deviate from the plan with consideration given to all facts and move forward with the implementation, or engage the CAB members for additional guidance.

Tasks to take place during implementation should be entered the tasks area and assigned to the resource who will be completing the tasks. That resource should notate and close the task when completed.

Be sure to enter a worklog for the amount of time spent on the change and by whom.

5.2.5 Step 5 System Testing

Every change should be tested post-implementation for accuracy and effectiveness, including by external users if required as part of the change.

- Scheduled Start: When testing is supposed to begin
- Scheduled End: When testing is supposed to end
- Actual Start: When testing actually began
- Actual End: When testing actually ended
- Include additional information such as testing plans and/or issues that came up during testing that either need to be addressed as part of the current change or should be considered for further investigation outside of the change.

5.2.6 Step 6 Review

Once the change is implemented and tested, verify all information of the change is complete. Ensure the change met the plan, implementation and timeline of the intended change. Enter a description as necessary.

5.2.7 Step 7 Close

All change steps are completed, worklog is filled in and all associated tasks throughout every stage are closed.

Indicate which of the following closure codes is appropriate based on the outcome of the change:

- **Closed – Approved**: Change that is closed immediately after approval, but not implemented.
- **Closed – Canceled**: Change that was canceled due to lack of desire to implement or requester changed their mind.
- **Closed – Completed**: Change that is closed after successful completion.
- **Closed – Deferred**: Change that is closed due to being put on hold.
- **Closed – Rejected**: Change that is closed due to rejection.

5.3 Emergency Changes

An emergency change is a change that must be introduced as quickly as possible. If the change is not implemented, the discovered issue will leave the County with significant financial, legal or security risk.

An emergency change is not a change that needs to be implemented because it did not go through the CAB approval process.

All emergency changes need to be approved by the Change Manager and either the CIO or Deputy CIO.

Emergency changes must have an associate incident request, if applicable. This is to ensure the change has a full description and history log that can later be reviewed.

The first priority of an emergency change is to restore services that are impacting as customer. A change record can be recorded retroactively if the emergency change is imminent. The goal of an unplanned emergency change is to restore services first, then record the change after implementation. If the emergency change is planned, the change should be recorded first and approved by the two appropriate emergency review members.

If the planned emergency change occurs during normal business hours, the change owner should coordinate a Teams meeting to call the emergency approvers in for review and approval.

If the emergency is off hours, the impacted manager of the team has the authorization to approve the planned emergency change if comfortable doing so. If needed, the manager can reach out to the Deputy CIO or CIO for additional guidance.

For all unplanned and planned emergency scenarios, the recommended action is for the change owner to have a Teams meeting to discuss change details prior to implementation.

6. Roles and Responsibilities

All OIT staff and third party vendors are expected to be familiar with and adhere to the contents of this policy and procedures.

CAB Members, may include all or any of the following:

- Chief Information Officer
- Deputy Chief Information Officer
- Infrastructure Manager
- Business Systems Manager
- Security and Continuity Manager

Change Manager – Department manager responsible to review and approve all proposed changes before CAB review.

Change Requester – The customer, either internal or external, who initiates the RFC.

Change Owner – The OIT resource with primary responsibility to coordinate/monitor the execution of the change and document the change within ServiceDesk Plus.

7. Definitions

Change: The addition, modification or remove of anything that COULD have an impact on services. The scope includes changes to IT production services and any related items.

Change Management: The process for controlling the lifecycle of changes.

Request for Change (RFC): A RFC is a request within ServiceDesk Plus for a proposed change.

Change Window: A timeframe when changes may be implemented with minimal impact on IT services.

Normal Change: A change that must follow the complete change management process. A normal change does not need to be immediately introduced.

Emergency Change: An emergency change must be introduced as soon as possible, in most cases, to resolve a major incident.

Change Advisory Board (CAB): The CAB is made up of leaders responsible for the assessment, prioritization, approval and scheduling of changes.

8. Policy Compliance

8.1 Compliance

This policy will be monitored and enforced by the Chief Information Officer (CIO), Deputy Chief Information Officer (DCIO) and department managers. Vendors are also expected to follow the OIT change management policy. Employee violations will result in coaching and repeat offenses may result in disciplinary action up to and including termination.

8.2 Exceptions

There are no exceptions permitted to the policy or procedures itself except for the following:

Any exceptions/challenges to an unsuccessful change must be brought forth to the CAB. The CAB members will make the final determination on whether or not a change is successful.