| | | | |
|---|---|---|---|
| **Policy Title:** | **Change Management Policy** | | |
| | Office of the Chief Information officer | **Category** | Information Technology |
| | | **Administrative Policy #** | |
| | | **Revision #** | N/A |
| | | **Review Frequency** | As Needed – no less frequently than triennially |
| **Administrative Division** | Information Technology Services | **Reviewed By** | Chief Information Officer |
| **BOWC Approval** | | **Last Reviewed/Update Date** | 7/2/19 |
| **Implementation Date** | | | |

## 1. OBJECTIVES

1.1. This change management policy is designed to ensure that standardized best practice methods and procedures are used for efficient and prompt handling of all changes, in order to minimize the impact of change-related incidents upon service quality, and consequently improve the day-to-day operations of the organization.

## 2. PURPOSE

2.1 The purpose of this policy is to define a consistent approach to manage changes to the IT environment at DWSD.

## 3. DEFINITIONS

“Backout Plan” means a plan, specific to the change control, that allows the change to be rolled back without damage to the hardware or software that is the subject of the change control

“Change Advisory Board” (CAB) is a cross-functional team responsible for assessing change requests in terms of business need, cost/benefit, viability, and potential impacts to existing systems or processes.

“Change Control” means the request and related information (including approval or denial) to make changes to hardware or software within the scope of this policy

“Change Management Procedure” means the documented steps to take to process a change control from initial request through completion or denial

“Service Development Life Cycle (SDLC)” refers to the standards around the creation of new services and standard updates, which includes the collection and documentation of requirements, design of a new system or update, development procedures, testing protocols, and deployment into production environment

## 4. SCOPE

4.1. This policy applies to all changes to hardware and software.

## 5. RESPONSIBILITIES

### 5.1. Chief Information Officer (CIO)

5.1.1. The Chief Information Officer (CIO) is responsible for publishing this policy; communicating this policy to all employees; for review, approval, and publishing of divisional standards, and for updating this policy as necessary.

5.1.2. The CIO, or delegate, is responsible for interpreting and enforcing this policy; ensuring that information resource usage is in compliance with Departmental policies and standards.

5.2. **Change Initiator**

5.2.1. The change initiator can be anyone in the Information Technology (IT) Department. This person is responsible for filling out the request for change, obtaining approval, and submitting the request according to the change management process.

5.3. **Change Manager**

5.3.1. The Change Manager has overall management responsibility for the change management process in the IT Group.

5.3.2. The Change Manager is responsible for oversight of the entire change process, conducting Change Advisory Board meetings, reporting and escalation of issues with the process.

5.3.3. The Change Manager is responsible for developing plans of action and milestones documenting the planned, implemented, and remedial actions and measures to correct any deficiencies during the assessment of change controls to reduce any risk.

5.3.4. The Change Manager is responsible for monitoring of related key performance indicators (KPIs).

5.4. **Change Approver**

5.4.1. The change approver is the manager who is responsible for the hardware or software that is the subject of the change.  The change approver signs off on the change before it goes to the change advisory board

5.5. **Change Advisory Board (CAB)**

5.5.1. The CAB reviews all change requests and decides whether to approve, defer, return, reject, or cancel changes and assigns a priority. Also, the CAB makes recommendations to the Change Manager related to change implementation.

5.6. **Emergency Change (EC) Authorizer**

5.6.1. This team (or individual) is a subset of the CAB that is responsible for dealing with emergency changes. The CAB/EC must be able to meet on a very short notice and authorize or reject changes with emergency priority.

5.7. **IT Policy Committee**

5.7.1. The IT policy committee is responsible for annually reviewing this procedure and for updating it as needed.

## 6. POLICY

6.1. No changes to hardware, communications equipment and software, system software and applications software in production environments shall be made without an authorized change control.

6.2. All authorized changes shall be made following the approved change management procedure as defined in section 6.6 below. All changes that impact access to or the performance of a user system will include a communication to the user community.

6.3. No non-emergency change control shall be authorized that does not have a backout plan.

6.4. The Change Manager will issue change management reports as requested by the Chief Information Officer (CIO).

6.5. The following change types are recognized:

6.5.1. Standard changes shall be submitted at least a week in advance, for discussion and approval (or rejection) at the weekly CAB meeting.

6.5.2. Business as usual (BAU) changes are pre-defined, standard changes that are documented, but do not need approval.

6.5.3. Expedited changes are submitted in advance of making the change, with relatively short notice, typically for break/fix situations. These changes require approval.

6.5.4. Emergency changes, submitted after the fact, after receiving verbal approval from an Information Technology manager, typically for emergency break/fix situations.

6.6. General procedures are as follows:

6.6.1. Standard changes and BAU changes – changes are submitted to the CAB for discussion and approved by the CAB at a weekly meeting.

6.6.2. Expedited changes – changes are submitted to the CIO for review, approved by the CIO or delegate, and scheduled for deployment as soon as possible without interrupting business operations. Expedited changes are discussed at the next meeting of the CAB.

6.6.3. Emergency changes – submitted to the CIO, approved by the CIO or delegate, and scheduled for deployment as soon as possible. Emergency changes are discussed at the next meeting of the CAB.