POLICY 040/2016 RAADSBELEID

MUNICIPALITY DAWID KRUIPER MUNISIPALITEIT

SUBJECT/ONDERWERP: **IT CHANGE MANAGEMENT POLICY**

REFERENCE/VERWYSING: **6.1.3.B**

RESOLUTION NR/BESLUIT NO: **17.8/11/2016 (CM)**   DATE/DATUM: **25 November 2016**

PURPOSE: This policy is to establish management direction and high-level objectives for change management and control. This policy will ensure the implementation of change management and control strategies to mitigate associated risks such as:

- Information being corrupted and/or destroyed;
- Computer performance being disrupted and/or degraded;
- Productivity losses being incurred; and
- Exposure to reputational risk

POLICY PHILOSOPHY AND PRINCIPLE

Changes to information resources shall be managed and executed according to a formal change control process. The control process will ensure that changes proposed are reviewed, authorised, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored

GUIDELINES

1.   System change is the result of one or several of the following factors:

- Policy or legislation change necessitating system change of input or output;
- System enhancement not originally envisaged in the design phase;
- User requirement changes;
- Errors in system design and or development.

2.   A request for change in a software system must be documented and contain the following minimum requirements:

   a.   Name of requesting Department
   b.   Name of requester
   c.   Full description of change required
   d.   Reason for change

   Wherever practicable, operational and application change control procedures should be integrated.

3.   All change requests shall be submitted to the IT Steering Committee for approval. The approval of all change requests and the results thereof shall be documented.

4.   An impact assessment shall be conducted which includes the potential effect on other information resources and potential cost implications. The impact assessment should, where applicable consider compliance with legislative requirements and standards.

5.   All change requests shall be prioritised in terms of benefits, urgency, effort required and potential impact on operations.

6.   Changes shall be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimise the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made.

7.   The impact of change on existing SLA's shall be considered. Where applicable, changes to the SLA shall be controlled through a formal change process which includes contractual amendments.

8.   All users, significantly affected by a change, shall be notified of the change when completed.

9.   The requester of the change shall sign-off on the change.

10.   Where applicable the business continuity plans shall be updated with relevant changes

11.   An emergency change is classified as a change that will seriously effect the outcome of the system if not done as soon as possible. To ensure the proper control, authorisation, and documentation of emergency changes the IT Steering Committee will approve the change at their next meeting.

PROCEDURE
1.   Change requests will be completed on the System Change Request form.

2.   The IT Manager will investigate the impact of the change on systems and make a recommendation to the IT Steering Committee.

3.   The IT Steering Committee may approve or decline the request.

4.   After approval the IT Manager will submit the request for change to the relevant service provider. The IT manager will monitor the change until such time that it is implemented.

5.   After implementation and testing, the requesting department will sign-Off on the change.

ROLES
IT Steering Committee
IT Manager
End users

RELATED POLICIES

REPEALS
Any previous policy or procedure prior to this policy is hereby recalled.