POLICY 036/2015 RAADSBELEID

ONDERWERP/SUBJECT: IT CHANGE MANAGEMENT POLICY

VERWYSING/REFERENCE: 6.1.3

BESLUIT NR/RESOLUTION NO: 16.14/12/2015

DATUM/DATW: 3 Desember 2015

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 PRINCIPLES

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, authorized, 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. Changes are classified in the following categories measured in accordance with the impact the change has on the system as whole and the risk factor if not implemented.

CATEGORY	DESCRIPTION
1	Cosmetic in nature - changes such as improving user friendliness of screens or reports, rectifying minor errors.
2	Policy or legislation changes enforcing system changes.
3	New features or additions / enhancements to system or major system changes.

3. System changes must be documented.

4. Changes are approved and reported as follows:

CATEGORY	
1	Approved by IT Manager and reported to the next IT Steering Committee
2	Approved by IT Manager and reported to IT Steering Committee
3	Approved by IT Steering Committee

Changes with high risk to council not reaching objectives or seriously effect the outcome of the system if not done as soon as possible and cannot wait for next IT Steering Committee meeting for approval, may be approved by the Chairperson of IT Steering Committee and reported to the next IT Steering Committee

5. 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.

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

7. 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.

8. To minimize any interruptions in system performance as a result of malfunctioning changes, backups be done prior to implementation to allow for rollback to original state.

9. Access control measures at all times be monitored and implemented.

10. 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.

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

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

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

PROCEDURE

1. The official requesting a system change completes a System Change Request form which must be duly signed by the Departmental Head and Director to whom he/she reports.

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