BERGRIVIER MUNICIPALITY

CHANGE CONTROL POLICY

CHANGE MANAGEMENT POLICY

REVISION NUMBER	DATE	AUTHORISED FOR DISTRIBUTION
1	27 February 2017	

1. INTRODUCTION

The Information Resources infrastructure at Bergrivier Municipality is expanding and continuously becoming more complex. There are more people dependent upon the network, more client machines, upgraded and expanded administrative systems, and more application programs. As the interdependency between Information Resources infrastructure grows, the need for a strong change management policy is essential.

From time to time each Information Resource element requires an outage for planned upgrades, maintenance or fine-tuning. Additionally, unplanned outages may occur that may result in upgrades, maintenance or fine-tuning.

Managing these changes is a critical part of providing a robust and valuable Information Resources infrastructure.

2. LEGISLATIVE FRAMEWORK

The policy was developed with the legislative environment in mind, as well as to leverage internationally recognised ICT standards.
The following legislation, amongst others, were considered in the drafting of this policy:

- Constitution of the Republic of South Africa Act, Act No. 108 of 1996;
- Copyright Act, Act No. 98 of 1978;
- Electronic Communications and Transactions Act, Act No. 25 of 2002;
- Minimum Information Security Standards, as approved by Cabinet in 1996;
- Municipal Finance Management Act, Act No. 56 of 2003;
- Municipal Structures Act, Act No. 117 of 1998;
- Municipal Systems Act, Act No. 32, of 2000;
- National Archives and Record Service of South Africa Act, Act No. 43 of 1996;
- Promotion of Access to Information Act, Act No. 2 of 2000;
- Protection of Personal Information Act, Act No. 4 of 2013;
- Regulation of Interception of Communications Act, Act No. 70 of 2002; and
- Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005.

The following internationally recognised ICT standards were leveraged in the development of this policy:

- Western Cape Municipal Information and Communication Technology Governance Policy Framework, 2014;
- Control Objectives for Information Technology (COBIT) 5, 2012;
- ISO 27002:2013 Information technology — Security techniques — Code of practice for information security controls; and
- King Code of Governance Principles, 2009.

3. OBJECTIVE OF THE CHANGE MANAGEMENT POLICY

The purpose of the Change Management Policy is to manage changes in a rational and predictable manner so that staff and stakeholders can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the information system of Bergrivier Municipality and to increase the value of Information Resources.

The Bergrivier Municipality Change Control Policy applies to all individuals that install, operate or maintain Information Resources.

4. THE AIM OF THIS POLICY

The aim of this policy is to ensure that the Municipality conforms to standard change controls in such a way that it achieves a balance between ensuring legislative compliance, best practice controls, service efficiency and that risks associated to the management of user access are mitigated. This policy supports the Municipality's Corporate Governance of ICT Policy.

5. SCOPE

Change Management: The process of controlling modifications to hardware, software, firmware, and documentation to ensure that Information Resources are protected against improper modification before, during, and after system implementation.

Change:

- any implementation of a new functionality
- any interruption of service
- any additional functionality
- any repair of existing functionality
- any removal of existing functionality

6. POLICY STATEMENTS

- Information security requirements must be included in the requirements definition when developing new information systems or when acquiring off the shelf software. The development and selection of software must consider these information security requirements, unless compensating controls can be implemented to address the perceived information security risks.
- All changes to information systems (including infrastructure and networks) will be controlled through change control. This will include the following controls, at a minimum:
  (a) All change requests must be logged, and monitored by the systems administrators, and approved by the relevant Senior Manager.
  (b) All changes will be documented, archived and permission for changes given to relevant service providers in writing.
  (c) All change requests must be reviewed by the relevant systems administrators, before the approval by the relevant senior manager. Major changes with a potential security or systems availability (down time) possibility must be identified as critical.
  (d) With critical changes service providers must provide test results to the relevant

systems administrators who must ensure that programs are well tested before the instruction is given to the service provider to deploy to the live environment.

(e) Emergency changes must follow the same process, only quicker. Documentation may be updated later- within a week.

(f) Critical changes must be tested in a secure test environment that is representative of the production environment by the service provider.

(g) The test environment must be separate from the production information systems.

(h) Critical changes must be tested by the service provider and test results must be submitted to the system administrator, prior to deployment.

(i) Critical change must be scheduled well in advance and must be performed in a planned manner to ensure success and fall back if required.

(j) Systems service providers will at all times be responsible, as per SLA, for the software as a system.

(k) Only systems service provider can deploy new or change programs to both the test and live environment.

- Test data must be protected in the same manner as production data, ideally by removing sensitive details beyond recognition. This is particularly relevant to data affected by legislation e.g. personal information.
- System Administrators must ensure that access to program source code and / or system documentation must be restricted to prevent the introduction of unauthorized functionality or disclosure of sensitive information.

7. DISCIPLINARY ACTIONS

Violation of this policy may result in disciplinary action. Additionally, individuals are subject to loss of Bergrivier Municipality Information Resources access privileges, civil, and criminal prosecution.

Annexure A

Bergrivier Change Control Form

Change Request #: ______________________ ***Project:*** _________________________

CHANGE REQUEST INITIATION: Originator: __________________ Phone#: (___)__________ email: ___________________

Date Submitted: ____/____/____ System/Product/Service Name: _________________________ Version Number: _________________

CONFIGURATION ITEM: Software: ___ Firmware: ___ Hardware: ___ Documentation: ___ Other: _______________

CHANGE TYPE: New Requirement: ___ Requirement Change: ___ Design Change: __ Other: _______________________

REASON: Legal: ____ Upgrade: ___ Patch: ___ Performance: ___ Customer Request: ___ Defect: ______ Other: ____________

PRIORITY: Emergency: ______ Urgent: ______ Routine: ______ ***Date Required:*** ____/____/____

CHANGE DESCRIPTION: *(Document and justify the request: the problems it resolves, the opportunities it creates, the policy it follows. Use attachment if necessary.)*

Attachments: Yes / No

TECHNICAL EVALUATION: *(Use attachment to explain changes, impact and on other entities, impact on performance etc.)*

Received By: ___________ Date Received: ___/___/___ Assigned To: _______________________ Date Assigned: ___/___/___

Type of Software/Hardware/etc. Affected____

Modules/Screens/Tables/Files Affected: ____

ESTIMATED COST: ______________

APPROVALS: Change Approved: ______ Change Not Approved: ______ Hold (Future Enhancement): ______

1. Head IT & Archives ____ Date: ____/____/____

2. Manager C.S ____ Date: ____/____/____

3. IT Committee ____

4. IT Committee Minutes as Change Order form (Attached): ___________ Date: ____/____/____

VERIFICATION OF CHANGE : *Name* __________________ Date: ____/____/____

UPDATE OF CONFIGURATION FILE : *Name* __________________ Date: ____/____/____

Annexure B

CHANGE REQUEST LOG

Content	Description
CR ID	
Short description	
Raised by	
Priority	
Date raised	
Owner	
Target date	
Status	□ Open □ Request for Technical review □Request further Analysis □ Approved □ Rejected □ Suspended □ Implemented □ Closed
Status date POE Attached	The date the status was last updated