GRAET KEI MUNICIPALITY

IT CHANGE MANAGEMENT POLICY

2023/2024

TABLE OF CONTENT

Details **Page No.**

1. OVERVIEW

The Information and Communication Technology environment dictates frequent change to applications, systems and overall infrastructure to ensure increased performance, functionality, security and reliability. However changes made to the system can also have an important impact on the functionality, usability and security of the system and surrounding systems. Therefore it is important to assess the impact of the change to existing system, document, approve and implement the change to manage possible negative outcomes.

A structured approach prior to change is needed to minimize the unexpected fall-backs. Management of change is critical to provide a strong and valuable ICT Infrastructure, applications to address the needs of the change.

The goal of a successful change management is reduce the amount of unplanned work as a percentage of total work done.

2. PURPOSE

Change Management procedure assists to manage in a balanced and expectable manner the change so that employees and third parties can plan accordingly. Change requires a serious planning, carefully monitoring and follow-up evaluation to reduce negative impact to the municipality's ICT resources and ability for users to perform their duties.

3. DEFINITIONS

Change Management: Is the process of controlling modification of software, hardware, firmware and documentation to ensure that ICT systems are protected against improper modification before, during and after system implementation

Change: Implementation of a new system/technology upgrade/update to existing systems and removal of existing system/technology functionality

Change Committee: a group of people involved in a change process

Policy: means IT Change Management Policy

Change Control Meeting: a meeting of the Change Committee to discuss, review, approve or reject Change Request

Change Requester: person who requests for a change

Change Requester Supervisor: Change Requester Supervisor

Change Implementer: person who coordinates the implementation of the requested

Change Coordinator IT: Is the representative from ICT

ICT/ IT Manager: Is responsible for ICT at the municipality

Client Representative: Is one person identified to coordinate the changes within the department/ section that requested the change.

Third Party (Service Provider): Is the vendor of the systems/technology that the change will be implemented to.

4. PROCEDURE

Each department working with the service provider of the applicable system or technology must document, authorize, test, approve and control all changes relevant to the appropriate system using the approved change process.

4.1 Change Management Request Form

- The manager should provide approval for the change after it was successfully tested.
- System must be backed up before implementing change.
- Data must be verified subsequently to change.
- Formal sign-off after successful upgrade, update to the change must be done.

4.2 **A change request must be submitted for all changes: both scheduled and unscheduled, in a timely manner to allow review and approval or denial of the change request, should include where applicable.**

- Justification/impact if change is not implemented.
- Contact information of the proposed change requester, change co-ordinator and Change Implementer where applicable.
- One person may perform more than one role: Changer Coordinator, Change Requester or Change Implementer.
- Change description, priority, cost involved if any, impact on client or service during and after change implementation and change Roll Back Plan.
- Identification of the risks of the change.
- Regulatory compliance benefits or issues (where applicable).
- Identification of the systems who may be impacted by the proposed change.
- Budgetary cost estimate of the change. (Where applicable).
- Test Plan (Where applicable)
- Success or failure of the proposed change.

4.3 **A change management log must be documented to generate, retain and review a record changes.**

- All change request must be logged whether approved or rejected on a standardised Change Request Form. The approval of the change request and the results thereof must be documented.
- A documented audit trail, maintained at Business Unit Level containing relevant information shall be maintained at all times. This should include change request documentation, change authorization and the outcomes of the change. No single person should be able to effect to production information systems without the approval of the authorised personnel.

4.4 **A procedure to address the emergency change requests.**

- Emergencies should be clear defined and exist only as a results of response to a natural disaster, or response to an emergency need.

4.5 **Email documentation must be attached as proof.**

5. TYPES OF CHANGES

All change requests shall be prioritised in terms of benefits, urgency, effort required and potential impact on business and ICT operations according to the following guidance:

5.1 Minor/Standard Change – A low-risk change with well-understood outcomes that is regularly made during the course of normal business. A Standard change follows pre-determined processes, is pre-approved and may be made at the discretion of the authorised personnel. Standard changes will be revised on an annual basis.

5.2 Major Change – A major change is one that has results in a change of mission critical information systems, it involves less understood risks, has less predictable outcomes, and/or is a change that is not regularly made during the course of business. Because of the ability to affect downstream or upstream business services, any proposed major change must follow a project management change process.

5.3 Emergency Change – this is similar to a major change, but must be executed with utmost urgency. There may be fewer people involved in the change management process review, and the change assessment may involve fewer steps, but any emergency change must be approved by the Staff and/or Line Function Manager and/or Senior Manager.

All system changes will abide by the process of classification and handling outlined in Error! Reference source not found..

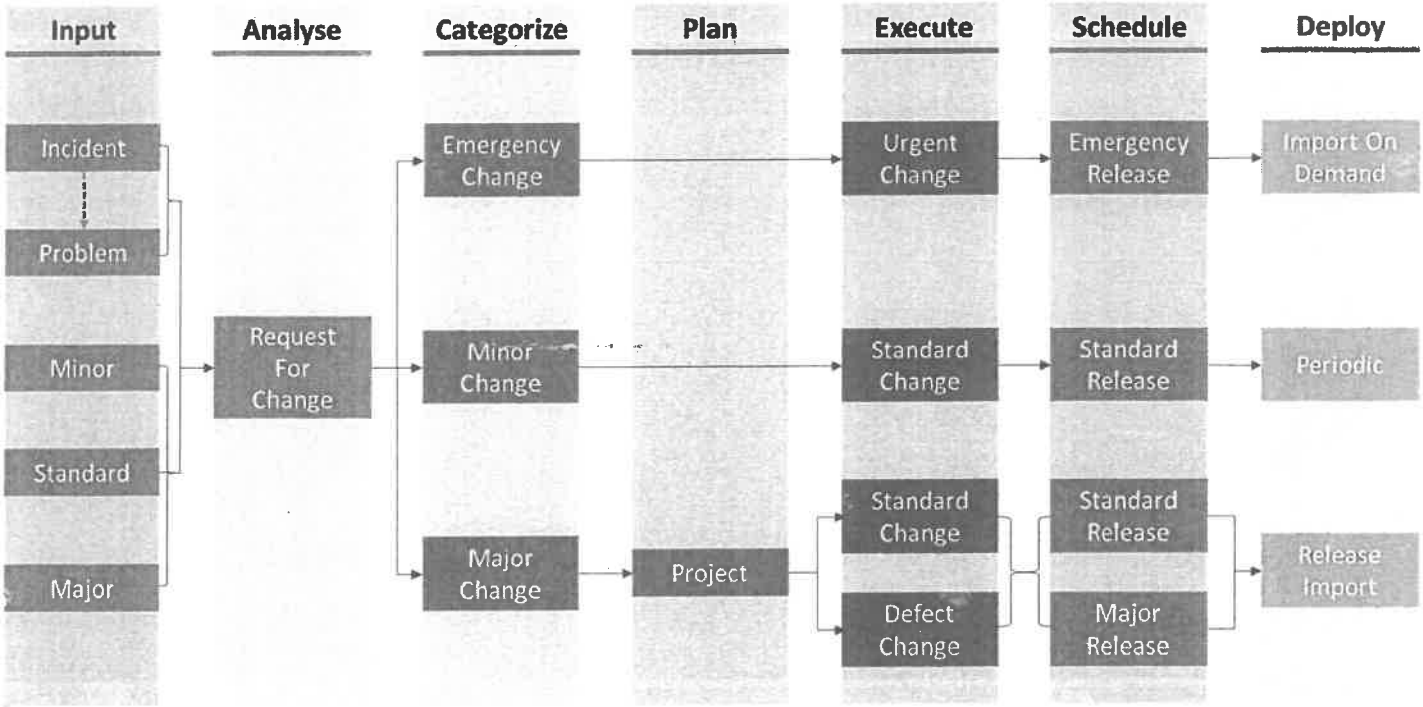

Figure 1: Change Model

All changes, except standard changes, should be planned and reflect as a minimum the following:

- What will be changed;
- Role-players and their responsibilities;
- When will the change take place;
- Implementation plan;
- Version control;
- Rollback plan; and
- Impact on the ICT Continuity Plan.

6. COMPLIANCE AND ENFORCEMENT

6.1 This policy may be partly or entirely abandoned or suspended by the Municipal Council on temporary or permanent basis.

7. SIGNATORIES

Signature of the Municipal Manager: _____

Date 29 June 2023

Signature of the Honorable Mayor: _____

Date 29 June 2023

GREAT KEI LOCAL MUNICIPALITY

PATCH MANAGEMENT POLICY

2023/2024

TABLE OF CONTENTS

1. PREAMBLE

WHEREAS The Municipality is responsible for ensuring the confidentiality, integrity, and availability its data that is stored on its systems.

WHEREAS The goal of vulnerability and patch management is to keep the components that form part of information technology infrastructure (hardware, software and services) up to date with the latest patches and updates.

WHEREAS Consequently, formal guidelines to regulate the patch management process are required.

NOW THEREFORE be it enacted by Council, as Patch Management Policy.

2. DEFINITIONS

2.1 DEFINITIONS

Name	Definitions
"Municipality"	Great Kei Local Municipality as determined by the Constitution of the Republic of South Africa Act No. 108 of 1996 Section 155 (1) (b).
"Municipal Manager"	The person appointed by council as the head of the administration of the municipal council as prescribed in terms of Section 54(A) of the Local Government: Municipal Systems Act No. 32 of 2000.
"User"	Councillor, or official who uses a municipal ICT working tool.
"Service providers"	Non- Great Kei Local Municipal employee's access to the network is subject to the security policy. Consultants employed in temporary or permanent capacity by Great Kei Local Municipality are classified as municipal employees for the purpose of this policy. Part time contractors and consultants who may have access to municipal facilities, infrastructure, systems and information will be required to sign a confidentiality and security undertaking. Also referred to as Third Party employees.

"Information security"	Information security encompasses the management processes, information is usable and can appropriately resist and cover from failures due to error, deliberate attacks or disaster; and that confidential information is withheld from those who should not have access to it.
"Access"	Physical or logical access to information or information system through a range of network devices.
"Information Security Officer"	An ICT professional within an organization responsible for providing technical support and maintenance of the information security infrastructure to ensure information assets and technologies are adequately protected.
"System Administrator"	An ICT professional within an organization responsible for providing system support and maintenance of the servers and transversal systems to ensure business continuity in the municipality.
"Anti-virus"	(software) designed to detect and destroy computer viruses.
"Computer virus"	A computer program that interferes with, or damages the normal operation of the computer or software. Virus programs are designed to infect other computers by hiding within e-mails or runnable programs
"Internet"	The municipality's internet shall be used as another delivery channel to offer communication and information to municipality constituents and potential constituents and, work related world wide web (www) access for employees.
"Email"	The Municipality supplied e-mail service is to make both external and internal work related communication more efficient and effective. Both internal and externally based browser (for example "outlook).

"Vendor"	A vendor, is an individual or company that sells goods or services to someone else in the economic production chain. ... Parts manufacturers are vendors of parts to other manufacturers that assemble the parts into something sold to wholesalers or retailers.
"Virtual Private Network"	A network that extends a private network across a public network, and enables users to send and receive data across shared or public networks.
"Firewalls"	A device/software that protects (a network or system) from unauthorized access.
"Patch Management"	An area of systems management that involves acquiring, testing, and installing multiple software updates (code changes) to an administered computer system.
"Hacking"	To gain unauthorized access to data in a system or computer.

2.1 Acronyms

ACRONYMS

ICT	Information and Communication Technology
IPS	Intrusion Prevention System
AV	Anti-virus

3. PURPOSE OF THE POLICY

3.1 To regulate maintenance of up-to-date operating system security patches on all Municipality owned and managed workstations and servers.

3.2 To define the procedures to be adopted for technical vulnerability and patch management.

3.3 To proactively prevent the exploitation of vulnerabilities on computing and related devices.

4. APPLICATION OF THE POLICY

4.1 This policy is applicable to all users whose computers are connected or linked to the Municipality network. This includes, but is not limited to, desktop computers (PC's), Laptop Computers, Servers, File/FTP/Proxy Servers and any hardware equipment that are suspect to virus or hacking attacks.

5. ROLES AND RESPONSIBILITIES

5.1 The Municipal Manager

The MM, working in conjunction with the directors shall be responsible for ensuring the effective implementation and compliance of this policy.

5.2 System owner (Head of the Directorate)

he designated owner of the system/ application shall approve the recommended system patches prior to deployment.

5.3 ICT Manager

5.3.1 The manager ICT must make a detailed formal recommendation to the Chief Financial Officer on the deployment of the latest patches.

5.3.2 The manager will also be responsible for ownership of all technical updates including: operating systems, patches for workstations and servers, antivirus and antispyware, drivers of devices.

5.4 ICT LAN Technician

5.4.1 The ICT LAN Technician , working with IT Desktop technician will be responsible for identifying patches for the application systems which they administer.

6. POLICY PROCEDURE

6.1 Many computer operating systems such as Microsoft Windows include software application programs that may contain security flaws. Occasionally, one of the flaws may permit an attacker to compromise a computer system.

6.2 A compromised computer system threatens the integrity of the network and all computers connected to that system. Almost all operating systems and many software applications have periodic security patches released by the vendor that need to be applied. Patches which are security related or critical in nature must be installed.

6.3 ICT will review, evaluate, and appropriately apply software patches in a timely manner. Should patches not be applied in a timely manner due to hardware or software constraints, mitigating controls must be implemented based upon the results of a risk assessment.

6.4 ICT must use automated tools, where available, to create a detailed list of all currently installed software on workstations, servers and other networked devices. A manual audit will be conducted on any system or device for which an automated tool is not available.

6.5 In the event that a system must be, reloaded, all relevant data on the current Operating System and patch level will be recorded. The system should be brought back to the patch levels in effect before reloading.

7. PATCHING PROCESS

7.1 Automated tools will scan for available patches and patch levels, which must be verified and installed accordingly.

7.2 Manual scans and reviews will be conducted on systems for which automated tools are not available.

7.3 Where feasible, patches will be successfully tested on non-production systems installed with the majority of critical applications or services prior to being loaded on production systems.

7.4 Successful backups of mission critical systems will be verified prior to installation of patches and a mechanism for reverting to the patch levels in effect prior to patching will be identified.

7.5 Patches will be applied during an authorised maintenance window in cases where the patch application will cause a service interruption for mission critical systems.

7.6 Reports will be generated for all system categories (servers, secure desktops or switches) indicating which devices have been patched. System reports help record the status of systems and provide continuity among administrators. The reports must be signed off and filed.

8. COMPLIANCE LEVELS

8.1 A compliance level refers to the percentage of computer devices that have been successfully patched or otherwise remediated such that they are no longer vulnerable.

8.2 Although a completely patched environment (100%) would be desirable, however, this does not take into account the reality of:

a) Users that own multiple computing devices (that are not always connected to the network or switched on).

b) Traveling employees with laptop computers who do not log into the municipal network every day.

c) Computers being repaired or replaced by hardware service providers.

d) Computers that may or may not even still exist on the municipal network, yet still show up on recent network inventory reports.

e) Failed or over saturated Wide Area Network connections.

f) Computers registered in Active Directory that have been recycled or re-imaged.

9. MONITORING

9.1 ICT division must monitor security mailing lists, review vendor notifications and Web sites, and research specific public Web sites for the release of new patches.

9.2 Monitoring will include, but not be limited to, the following:

- Scanning the Municipality's network to identify known vulnerabilities.
- Monitoring notifications, and Web sites of all vendors that have hardware or software operating on Municipality's network.

10. COMPLIANCE

a) The relevant Directors are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.

b) Any conduct that interferes with the normal and proper operation of the Municipality's ICT systems, which adversely affects the ability of other users to use those ICT systems, or which is harmful or offensive to other users, shall constitute violation of approved ICT policies.

c) The Municipality's management reserves the right to revoke the privileges of any user at any time.

11. APPROVAL OF THE POLICY

The Municipal Council must approve this policy and any amendment thereof.

12. REVIEWAL OF THE POLICY

This policy shall be reviewed annually.

13. AUTHENTICATION

This policy was adopted by Council on the _____

As per resolution Number _____

Signature of the Municipal Manager .....

Date 29 June 2023

Signature of the Mayor.....

Date 29 June 2023