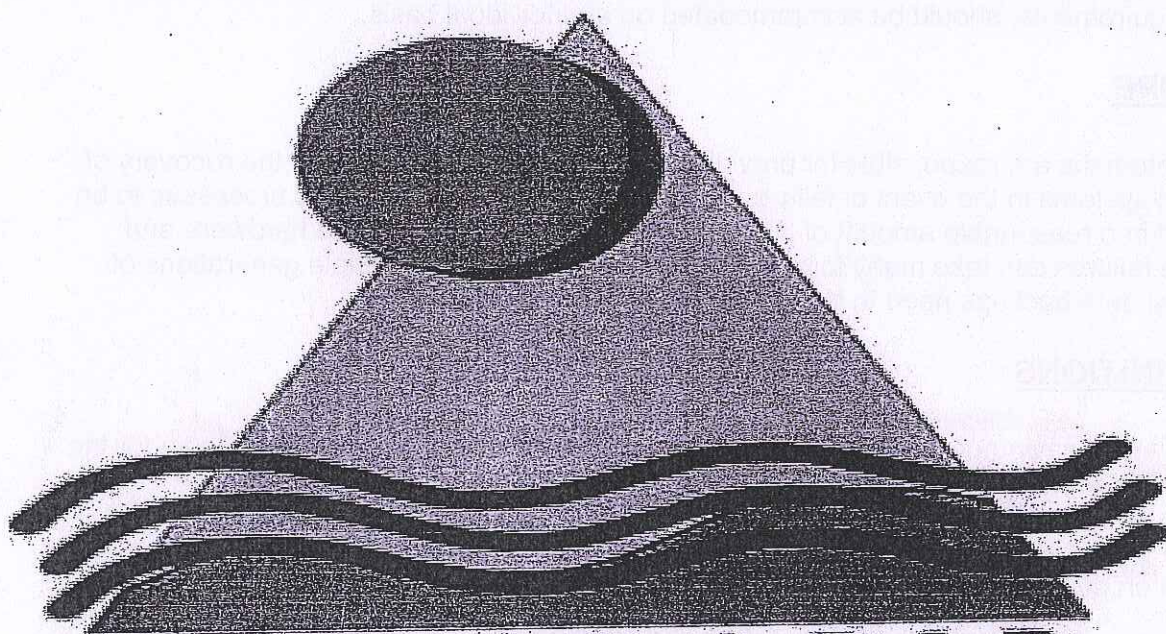


KAI !GARIB MUNICIPALITY



KAI !GARIB
MUNICIPALITEIT-MUNICIPALITY

BACKUP POLICY

1. OVERVIEW

This policy defines the backup policy for systems within the municipality which are expected to have their data backed up. These systems are typically servers but are not necessarily limited to servers. Servers and applications that are expected to be backed are detailed in section 6, system backup schedule.

2. PURPOSE

All electronic information considered of municipal value should be copied onto secure storage media on a regular basis (i.e., backed up), for disaster recovery and business resumption. This policy outlines the minimum requirements for the creation and retention of backups. Special backup needs, identified through technical risk analysis that exceeds these requirements, should be accommodated on an individual basis.

3. SCOPE

Data custodians are responsible for providing adequate backups to ensure the recovery of data and systems in the event of failure. Backup provisions allow business processes to be resumed in a reasonable amount of time with minimal loss of data. Since hardware and software failures can take many forms, and may occur over time, multiple generations of municipal data backups need to be maintained.

4. DEFINITIONS

Backup - The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

Restore - The process of bringing off-line storage data back from the offline media and putting it on an online storage system such as a file server.

Municipality Critical Data - Data that if it were deemed unavailable to the Municipality will have an immediate (within 24 hours) critical impact on the Municipality.

Data Owners - Department managers, members of the top management team, or their delegates who bear responsibility for the acquisition, development, and maintenance of production applications that process Municipality information.

Data Custodians - Are in physical or logical possession of either Municipality information or information that has been entrusted to them. Kai !Garib Municipality Custodians are responsible for safeguarding the information and making backups so that critical information is not lost.

FTP - (File Transfer Protocol) - Data is transferred from one department/computer to another over the internet.

5. POLICY

5.1. Regardless of classification, the availability of all data must be maintained by means of periodic back-ups and recovery mechanisms.

5.2. All data must be incorporated as part of a backup procedure.

5.3. Servers and systems will be backed up using a suitable backup method.

5.4. An appropriate storage medium will be used. This may be CD, tape, external hard drive, a mirrored server at a remote site, or any other recognised medium.

5.5. The IT Officer must monitor the status of all backups that are performed.

5.6. The backup status must be reviewed on a daily basis and any faults identified must be rectified.

5.7. It is the responsibility of each employee to ensure that his/her data is backed up regularly.



6. SYSTEM BACKUPS SCHEDULE

Application Frequency Performed By Storage Media Storage Location

Application	Frequency	Performed By	Storage Media	Storage Location
SEBATA FMS	Mon-Thu 21h00 pm – Incremental Retention - 1 Week Fri 21h00 pm – Full (Every 2nd week) Retention - 2 Weeks	IT Officer	KaiBackup NAS	Designated location (Known to all IT stuff)
IMIS SERVER	Mon-Fri 17h00 pm – Incremental Retention - 1 Week Sat 17h00 pm – Full (Every 2nd week) Retention - 2 Weeks	IT Officer	KaiBackup NAS	Designated location (Known to all IT stuff)
Domain Controller	Mon-Thu 19h00 pm – Incremental Retention - 1 Week Fri 19h00 pm – Full (Every 2nd week) Retention - 2 Weeks	IT Officer	KaiBackup NAS	Designated location (Known to all IT stuff)
File Server	Mon-Fri 23h00 pm – Incremental Retention - 1 Week Sat 23h00 pm – Full (Every 2nd week) Retention - 2 Weeks	IT Officer	KaiBackup NAS	Designated location (Known to all IT stuff)

7. RESPONSIBILITY

IT UNIT

The IT Officer shall perform regular backups. The delegated person shall develop a procedure for testing backups and test the ability to restore data from backups on a quarterly basis.

The Employee

All business critical data on local computer and notebook hard drives must be copied or moved to a share (H: drive) on a file server, where it will be backed up. Where such an action is not possible, as in cases where it is done away from access to Kai !Garib Municipality network, the data must be copied over on the first available opportunity. It will be the sole responsibility of the employee, under all circumstances, to backup and maintain security regarding personal data. Only document type files will be stored on the file server, e.g. .docx, .doc, .pdf, .xlxs, etc. Files that will be omitted are:

Users that require files to be restored must submit a request to the ICT Service Desk by completing the ICT Data Restore Request Form (see attached).

8. TESTING

The ability to restore data from backups shall be tested periodically by the IT Officer. Service Providers will also be required to perform backup testing as per the agreed upon SLAs.

7.1. Restoration and Testing of Backups

7.1.1. On a quarterly basis a restoration of one back-up from each system must be performed to ensure that back-ups can be restored in an effective and timely manner.

7.1.2. The restoration must be performed on a test environment to ensure that it does not impact on the production environment.

7.1.3. Documented evidence of the back-up restorations must be retained.

7.1.4. Users that need files restored must submit a request to the IT Officer. Include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

9. OPERATOR LOGS

9.1. The IT Officer will maintain an activity log and system reports for each system.

9.2. This will include:

9.2.1. System start/finish times, for planned downtime, unplanned downtime and system maintenance routines;

9.2.2. System error reports and corrective action taken; and

9.2.3. Operator identification (Initials) for each log entry.

10. BACKUP MEDIA STORAGE LOCATIONS

Back-ups of sensitive, critical, and valuable information must be stored in an offsite location, situated in an area where the possibility of the risk occurring at this site is minimal.

11. ENFORCEMENT

11.1. Non-compliance, violation and disregard of this policy shall result in disciplinary action and sanctions against the employee concerned and such sanctions may lead to termination of the employee's employment contract, depending on the circumstance and the gravity of the transgression.

11.2. In the event of Kai !Garib Municipality incurring financial loss as a result of noncompliance, violation and / or disregard of this policy, Kai !Garib Municipality shall be entitled to institute legal proceedings to recoup the loss it has incurred from the employee / user, and this shall be in addition to the disciplinary action that Kai !Garib Municipality would have taken against the employee.

K A I ! G A R I B