GREAT KEI MUNICIPALITY

BACK-UP POLICY 2023/24

- All software whether purchased or created personally is to be protected by at least one full backup.

- Each system data shall be backed up at least once a month.

- Data will be backed up to the file server, and it backs up as per licensed users.

3. POLICY STATEMENTS

- Backup copies of the files and program necessary to effect a recovery in the event of a disaster on server platforms should periodically be performed to safeguard the Authority's information and data.
- The backup media should have Disaster Recovery Site either cloud solution or on premises of the institution.
- Backups should be stored in a fireproof environment or safe. If no such environment exists; the tapes should be stored off-site.
- The success or failure of backups should be checked daily, investigated and corrective action taken if failure occurred.
- Backup reports are to be filed and kept for at least three months.
- Backups are to be scheduled to run during non-peak hours. Backup systems tend to have a negative effect on the speed of the network hence off-peak hours are recommended. Or should be scheduled opportunistic so whenever the node is connected to the network and back up process must take place.
- Backup media should not be used longer than the manufacturer's recommended life span (i.e. Backup tapes are not to be used more than the period recommended. Backup facility should not be used beyond the lifespan of licensing, backup licenses must be valid at all times.)
- Where backup procedures are inadequate or lacking, data may be lost or, effectively, unavailable, thus compromising the Authority's business processes and operations

4. DISASTER RECOVERY PROCEDURES

4.1 GENERAL

With the responsibilities that are entrusted on the Authority, the question of data integrity becomes paramount. Due to the growth of data that is handled by Authority, risks attached to various computing facilities highlight the need for a contingency plan.

4.2 OBJECTIVES

4.2.1 The primary objective of the document

- The primary objective of this document is to define a backup and recovery strategy to enable the Authority to recover from any disaster with minimum disruption to service in terms of business requirements and in a cost effective manner.
- To ensure that the recovery facility is reliable, effective and ready for use should network computers and servers suffer from a disaster.
- To ensure that proper resources and structures are in place to support the disaster recovery plan and identify shortcomings of the plan with a view to improve on it.
- To define and document critical activities and procedures to survive disaster.
- To empower the responsible Disaster Recovery Plan personnel and teams for their actions according to the procedures issued

4.2.2 Disaster definition

A disaster is a sudden, unplanned calamitous event that creates an inability on an organisation's part to provide the critical business functions for some predetermined period of time, which result in great damage.

Disaster can be divided into 3 main categories:

4.2.2.1 Minor

The loss of one or more user data files, or of a non - critical application. This type of disaster last for a short period of time and can be recovered in-house. This type often has less financial implications to organizations.

4.2.2.2 Major

The loss of disk, major hardware component or critical application. This type of a disaster lasts for longer period and might need extra support. Additional external assistance might be needed to address this disaster with added financial implications.

4.2.2.3 Catastrophic

The entire computer/server room is destroyed and computer equipment shall have to be completely replaced and software restored. This type can last longer, weeks or even months. The recovery process might have major financial implications to the organisation.

5. DISASTER DECLARATION

- The disaster declaration procedures must incorporate escalation procedures and clearly define what type of outages shall determine the procedures to be followed. It must define who has the authority and responsibility to declare a disaster.
- Once a disaster is declared, the recovery procedures shall immediately govern the recovery process.
- When the decision has been taken to invoke the disaster recovery plan, the control team shall meet to assess the extent of the damage and to formulate a recovery strategy (set out in section (8) below)
- There shall be disaster recovery IT coordinator whose function shall be to oversee the whole recovery process.
- A disaster shall be declared when a computer environment shall have a major impact on data integrity and halt the activities of the organization.

6. STRATEGIES

6.1 Disaster recovery strategy

- The Authority's recovery strategy shall be to recover all lost data within (24) hours from the time of the declaration of the disaster.

- If there is disk or other restrictions preventing the restoration of all data at once, only the most critical data and applications shall be restored

6.2 Backup strategy

- Backup of file and other servers shall be done from Mondays to Fridays.

- Backups shall be made on an external hard drive (DAT72 removable Tape cartridge). The size of the tapes to be used shall be determined from time to time by the Information Technology Section.

- After every backup, the results of each backup shall be studied daily using a log file and a record kept for future references. A screen shot must be done, signed and witnessed

- If backup fails it is to be resubmitted immediately. This is the only instance where backup shall be allowed to run during peak hours.

- The IT Officer or IT System administrator shall investigate the cause of failure and take corrective action. Measures shall be taken to avoid the repeat of the problem in the future.

7. DISASTER RECOVERY TEAM

The control team

- Team Leader – Municipal Manager
- Co-ordinator – Chief Financial Officer .
- Technical – ICT and Systems Administrator

Disaster Recovery Co-ordinator

Chief Financial Officer

8. FUNCTIONS OF THE ICT CONTROL TEAM

- The purpose of the team is to be available in a production server room and to implement the disaster recovery plan, and monitor the status of the recovery operations.
- The primary function of the control team is to assess the situation, co-ordinate and manage the recovery process of computer services.
- The control team co-ordinator shall oversee all activities involved and key decision making roles.
- Other functions of the control team may include arranging the finance of the recovery and advising the organization in order to assist in handling of any legal and public relations (media enquiries) matters, which may arise. In this instance communications team must be involved for the media briefings.
- The control team shall decide when the disaster shall be called off. The team shall also decide on a communication strategy to be used.
- The disaster shall be called off the moment the complete network is restored to its original state before the disaster occurred.
- The control team shall conduct a post mortem after the disaster has been called off. It shall implement a plan of how to prevent similar problems and, if required, amend the DRP, comparing it to the disaster it learnt from, to make future recovery process faster and more efficient.

9. ACTIVITIES OF THE CONTROL TEAM ACTIVITIES

- Assist in managing insurance claims adjustments.
- Begin evaluating recovery options.
- Maintain financing of recovery.
- Invoke plan for relocation if necessary.
- Schedule user relocation if necessary.
- Announce user relocation if necessary.
- Review transition plan.

10. RECOVERY STAGES

The following are guidelines of recovery stages in case of a disaster, depending on the nature of the disaster. These guidelines indicate possible problems that can occur and possible solutions that can be implemented.

10.1 Scenario 1:

Hardware

Hardware failure.

Replacement of components.

Recover backup from drives.

10.2 Scenario 2:

Network
Network failure;
Replace UTP cable; and

Network equipment failure. Install new equipment.

10.3 Scenario 3:

Hardware/Network
Hardware and network failures;

Replace servers/components;

Replace cables; and

Recover from backup.

11 ASSUMPTIONS AND CONTINGENCIES

11.1 Assumptions

This section contains some general assumptions, but does not include all special situations that can occur. Any special decisions for situations not covered in this plan needed at the time of an incident shall be made by senior management assisted by the ICT and Systems Administrator.

11.2 Incidents requiring action

This disaster recovery plan for the Authority shall be invoked if any of the following occurs:

- An incident, which has disabled or shall disable, partially or completely, the central computing facilities and networks for period of (24) hours.
- An incident, which has impaired the use of computers and networks, managed by the Authority, due to circumstances that fall beyond the normal day-to-day processing of data.
- An incident which was caused by problems with computers and networks managed by the Information Technology Section and has resulted in the injury of one or more employees of the Authority.

11.3 Contingencies

Potential dangerous situations to computer equipment:

- Power and air conditioning interruptions.
- Weather and natural phenomenon.
- Sabotage and interdiction.
- Fire.
- Water.

12. SIGNATORIES OF THE MUNICIPALITY

Signature of the Municipal Manager: _____

Date _____

Signature of the Honorable Mayor: _____

Date _____