POLICY 020/2015 RAADSBELEID

ONDERWERP: IT-DISASTER RECOVERY

VERWYSING: 6.1.B

BESLUIT NR: 26/05.1/2015 (SRV) DATUM: 13 Mei 2015

PURPOSE: This policy defines guidelines and procedures required to assist in minimizing the impact that a disaster would have on the operations of council being supported by IT resources.

POLICY PHILOSOPHY AND PRINCIPLE

//Khara Hais Municipality uses IT resources to assist in achieving objectives related to:

- Processes and activities of service delivery to the community
- Processes required for the administration of the organization

This policy serves in the identification of mission critical IT resources required to maintain these objectives and putting measures into place that will minimize the effect a disastrous situation would have on achieving the objectives of Council.

DEFINITIONS

"*Disaster*" Unforeseen situation that arises and if not managed will result that Council cannot achieve its objectives because employees are unable to perform their regular roles and responsibilities through the non –availability or –functioning of IT resources.

"*Disastrous events*" Disasters happen during one or more of the following events that impact on IT resources

1. Natural disaster

    i. Fire
    ii. Floods
    iii. Storms
    iv. Epidemic

2. Man made disaster

    i. War
    ii. Accidents
    iii. Technology failure

"*IT Resources*" Includes IT –system, -equipment, -technology and -personnel.

"*IT Disaster Recovery Plan (IT-DRP)*" Documented processes and procedures that must be followed to minimize the risk associated with a disaster

"*IT Disaster Recovery Centre (IT-DRC)*" A facility other than the normal place from which IT resources, operations and processes are driven and managed to which these are diverted should a disaster cause the normal place to be inadequate, unavailable or inaccessible.

GUIDELINES

1. A comprehensive IT-DRP must be established addressing processes and procedures in line with the guidelines set out in this policy to be followed in times of a disaster.

2. Processes requiring IT resources are classified within the Business Continuity Plan as follows:

Classification	Color Code	Description
Critical	Red	IT related processes and activities that are mission critical in achieving the councils objectives and cannot be delayed or stopped
Essential	Orange	IT related processes and activities required to reach councils objectives but can be delayed for a short period
Important	Yellow	IT related processes and activities required to reach councils objectives but can be delayed temporarily by using alternative methods
Value Adds	Green	IT related processes and activities required to reach councils objectives but can be delayed for longer periods.

3. For IT resources classified as "*Critical*", backup data, equipment and systems needs to be in place that can be activated or acquired within 12 hours that a disaster is identified.

4. For IT resources classified as "*Essential*", processes need to be in place to activate or acquire backup data, equipment and systems within 36 hours that a disaster is identified.

5. For IT resources classified as "*Important*" and "*Value Adds*", processes need to be in place to activate or acquire backup data, equipment and systems as soon as possible after a disaster is identified.

6. A suitable location must be identified and equipped to serve as the IT Disaster Recovery Centre.

7. Locations other than the normal location of business operations must also be identified and equipped with resources that link to the IT-DRC from which mission critical operations can be continued in the event that business processes cannot be performed from the normal place of business due to a disaster.

8. All IT related data must be backed up and stored in line with the IT backup policy for use during a disaster situation.

9. Disaster recovery teams must be established and personnel appointed with clear instructions and procedures to enable continuity of IT resources and business processes.

10. The IT-DRP must be tested at least once every 12 months

11. A disaster is registered when a disastrous event is the cause that:

    a. One or more IT resources are non-functional,
    b. The building or facility utilized for council processes is not available for an extended period of time

12. Where a registered disaster affects processes using IT resources, the IT-DRP is activated.

PROCEDURES

1. The IT Manager establishes a IT-DRP that is signed-off by the IT Steering Committee.

2. Heads of Departmental assist the IT Manager in classifying IT resources by means of completing a Business Continuity Plan of all processes within their applicable department.

3. The IT Manager identifies a suitable location to serve as IT-DRC and is signed-off by the IT Steering Committee for establishment.

4. The IT Manager must establish disaster recovery teams of different expertise within the IT establishment with defined tasks and responsibilities to run the IT-DRC and rectify failures caused by a disaster.

5. Heads of Departments must identify locations from which mission critical operations are to be performed in times that business operations cannot be performed from the normal place due to a disaster.

6. The IT Manager ensures that the IT-DRP is tested at least once in a 12 months cycle.

7. The Municipal Manager will declare a disaster and report on activities and progress to Council.

8. The Director Corporate Services will act as the IT Disaster Manager and report on activities to the Municipal Manager.

9. The IT Manager and his team will activate the IT-DRC once a disaster is declared.

10. Heads of Departments identify employees to maintain business operations once a disaster is declared.

ROLLs

Municipal Manager
Directors
IT Manager
Heads of Departments
Nominated Staff

RELATED POLICIES

Business Continuity Policy
IT Backup Policy

RECALL / CHANGE

This policy replaces any previous policy in this regard.