POLICY 039/2016 RAADSBELEID

MUNICIPALITY DAWID KRUIPER MUNISIPALITEIT

SUBJECT/ONDERWERP: **IT BACKUP POLICY**

REFERENCE/VERWYSING: **6.1.3.B**

RESOLUTION NR/BESLUIT NO: **17.7/11/2016 (CM)** DATE/DATUM: **25 November 2016**

PURPOSE: This policy is designed to prevent critical data of Dawid Kruiper Municipality being lost and ensure it can be recovered in the event of an equipment failure, intentional or unintentional destruction of data or disaster.

PHILOSOPHY AND PRINCIPLES

Information and data is generated on various systems and applications used within Dawid Kruiper Municipality. To prevent the loss of data due to accidental deletion or corruption of data, system failure, or disaster it should be timeously backed up and secured for restoration and thereby minimize the impact on business and /or service delivery. This policy applies to all data on equipment owned and operated by Dawid Kruiper Municipality.

GUIDELINES

1. 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.

   Archive - The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.

   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.

   IT - The Information Technology department of Dawid Kruiper Municipality

2. Backup media - Backups are done on one of the following media:

   2.1 Tape.
   2.2 Mass storage USB device.
   2.3 Network adapted storage (NAS).
   2.4 Hard drive of another PC (departmental only).

3. System backups

   Full backups of system data are performed nightly on Monday, Tuesday, Wednesday, Thursday, and Friday. The following applies:

   3.1 A separate backup for each day including Monday, Tuesday, Wednesday, and Thursday. Backups performed Monday through to Thursday shall be kept for one week and used again the following appropriate day of the week

   3.2 A separate backup for each Friday of the month such as Friday1, Friday2, etc. Backups performed on Friday shall be kept for one month and used again the next month on the applicable Friday.

   3.3 A separate backup for year-end on 30 June. Backups performed on year-end shall be kept for two consecutive years and the oldest be used again the third year

3.4 Storage of backup data

Media will be clearly labeled and stored in a secure area that is accessible only to IT-staff, staff responsible for backup or employees of the contracted secure off-site media vaulting vendor.

3.4.1 Daily backups will be stored on-site in a physically secured fire-proof safe located in a building separate from the location of the server.

3.4.2 Weekly and year-end backups will be stored in a physically secured, off-site media vaulting location maintained by a third party.

4. User data residing on PC's or Laptops

4.1 Incremental backup of user data performed nightly on Monday, Tuesday, Wednesday, Thursday, and Friday

4.2 When a backup cannot be performed due to equipment not being switched on or attached to the network, such backup will be performed during the day at the next sign-on.

4.3 User data backup will reside on NAS media.

5. Storage media consistency

5.1 Magnetic tapes

5.1.1 The date each tape was put into service shall be recorded on the tape.

5.1.2 Tapes used daily and weekly are used for no longer than six months and shall be discarded and replaced with new tapes.

5.1.3 Tapes used for year-end are discarded and replaced every six years.

5.1.4 Tape drives must be cleaned weekly using a cleaning tape.

5.1.5 Tapes retracted from service must be formatted and disposed of as per hazardous material disposal policy.

5.2 USB and drive storage devices

5.2.1 A check disk must be done weekly on the device to ensure no bad sectors are found. Disk containing bad sectors are discarded and replaced with new disks.

5.2.2 Check disk scan information must be recorded.

5.2.3 Disc retracted from service must be formatted and disposed of as per hazardous material disposal policy.

5.3 The IT-Department will at regular intervals check logged information generated from each backup job to investigate for and correct errors. IT will identify problems and take corrective action to reduce any risks associated with failed backups.

6. Disposal and retirement of media

6.1 Prior to retirement and disposal, IT will ensure that:

6.1.1 The media no longer contains active backup images.

6.1.2 The media's current or former contents cannot be read or recovered by an unauthorized party.

6.2 With all backup media, IT will ensure the physical destruction of media prior to disposal.

7. Data to be backed up

7.1 All system data residing on a server owned or in control by Dawid Kruiper municipality must be backed up in accordance with this policy.

7.2 All files of type document, spread sheet, presentation, pdf, drawings, mails, etc. containing information with regard to Dawid Kruiper business or in communication to or from Dawid Kruiper Municipality residing on a PC, Laptop or other electronic device must be backed up in accordance with this policy.

8. Data restore testing

The content of a backup media must be tested monthly to ensure that it can be restored.

9. Responsibility for backups

9.1 The IT-System Administrators is responsible to ensure that backups are done for all server data residing and in control of the IT-Department

9.2 For any server not in control of the IT-Department, the Departmental Head of the department were a server is housed must appoint someone to make backups.

9.3 Users of PC' s are responsible to ensure that the PC' s remain powered on after hours so that the automated backup can run.

9.4 Users of Laptops must ensure that the laptop is connected to council's network for at least one day per week so that the automated backup can run.

10. Restoring and recovery of data

10.1 Requests for restoration of information will be made to the help desk and a request form completed.

10.2 In the event of a catastrophic system failure, the latest backup information will be made available as soon as the destroyed equipment has been replaced.

10.3 In the event of a non-catastrophic system failure or user error, the latest backup information will be made available.

PROCEDURES

1. When system backups are made to a tape drive or USB mass storage device:

1.1 The chosen media are labeled and the date of first time use is recorded thereon.

1.2 Daily backups

1.2.1 A set of four media are marked Monday, Tuesday, Wednesday and Thursday.

1.2.2 Every morning the previous day’s media is removed/ unplugged and a media corresponding to the current day is inserted into the drive or connected.

1.3 Weekly backups

1.3.1 A set of five media are marked Friday1, Friday2, Friday3, Friday4 and Friday5.

1.3.2 Every Friday the previous day's backup media is removed/ unplugged and a media corresponding to the Friday of the month is inserted into the drive or connected. (first Friday of month = Friday1, second Friday = Friday2, etc.).

1.4 Year-end backups

1.4.1 A set of two media for year-end are kept and labeled to correspond with the year it will be used. Each media will be used every second year (eg. 2012, 2014, 2016, 2018, 2020).

1.4.2 Every year on 30 June the previous day's backup media is removed/ unplugged and the media corresponding to the year is inserted into the drive or connected.

1.5 When a tapes lifetime expires or a USB storage device has bad sectors, the media is handed to IT to destroy and dispose of in accordance with policy.

1.6 The backup register is completed daily contains the following information:

1.6.1 Date and day.
1.6.2 Person replacing media name and signature.

2. When system backups are made to NAS storage devices:

2.1 The IT-Department will create separate directories for each system of origin named clearly for reference purposes.

2.2 For daily backups

2.2.1 Each directory will have subdirectories named Monday, Tuesday, Wednesday, Thursday and Friday.
2.2.2 A scheduled task is created to daily backup data to the corresponding subdirectory.

2.3 For monthly backups

2.3.1 Each directory will have subdirectories named monthly
2.3.2 A scheduled task is created to monthly backup data to the corresponding subdirectory.

2.4 For yearly backups

2.4.1 Each directory will have subdirectories named yearly
2.4.2 A scheduled task is created to yearly backup data to the corresponding subdirectory.

2.5 Every Monday a printout of the scheduled history is printed and filed.

3. For the backup of user info

3.1 The IT-Department will create a scheduled task to run after hours. This is done to minimize traffic on the network.

3.2 It is the user's responsibility to ensure:

3.2.1 PC remains switched on after hours.
3.2.2 Laptops are connected to the network at least once per week.

ROLES
Staff from IT-Department, All employees using IT-related equipment.

RELATED POLICY
Disposal of Hazardous IT-related waste.

REPEALS
Any previous policy or procedure prior to this policy is hereby recalled.