ANNEXURE F:

IT DISASTER RECOVERY PLAN

[CS]: REVIEW OF IT FRAMEWORK

COMPETENCY: MAYORAL COMMITTEE

PURPOSE:

To submit the reviewed IT Framework for approval.

RECOMMENDATIONS:

1. That the reviewed IT Framework which deals with the following matters, BE APPROVED:

    (i) Back-up Policy (Schedule 1).
    (ii) Disaster Recovery Strategy (Schedule 2).
    (iii) Terms of Reference for I T Steering Committee (Schedule 3).
    (iv) Standard Operation Procedure: Access to Systems and Controls (Schedule 4).
    (v) Review of IT Functions (Schedule 5).
    (vi) Review IT policies (Schedule
        6) IT Usage Policy;
        IT Access Policy, IT
        Security policy;
        IT Change management policy;
        IT Laptop policy
        IT Charter and
        MLM Master systems plan.
2. That the IT Framework be reviewed annually by the Section 80 Corporate and Finance Services Portfolio Committee, with a report to the Mayoral Committee if significant changes are required or envisaged.

REPORT

Attached hereto is the reviewed IT Framework which has been updated and addressed in terms of the Auditor – General requirements and suggestions. It will be submitted to the Auditor – General's office to establish whether any possible shortcomings still exist. It will also be reviewed annually.

SCHEDULE 1

MIDVAAL LOCAL MUNICIPALITY BACKUP POLICY

Systems Backup

1.1 Frequency and Timing of Backups

1. A backup is taken every day.
2. Backups are scheduled to run every day commencing at 18h00.
3. Month-end backup is taken monthly after the financial month-end procedures.
4. Year-end backup is taken annually after the financial year-end procedures.
5. Backups are taken by doing a Disk to Disk backup on the host server. Once this backup is completed a backup is then done to the Sep Sesam server (Disk to Disk). The following day this backup is the written to a DLT tape to be kept in the safe storage environment.
6. The replication of the core systems to the DRP server is done daily after the backups have been completed. There is thus more than one backup done of the core systems on a daily basis.

1.2 Backup Procedure

1. Changing tapes according to schedule: inserting tape at close of day and removal of tape from the backup unit after migration from disk to tape is done..
2. Storing the backup tapes in fireproof safe.
3. Checking that the backup has been successful.
4. Managing a backup failure.
5. Maintaining the backup log.

1.3 Verification of Backup Status

1. The designated member of staff must check the backup status on the system daily and report any failures to the Administrator.
2. Proof of successful backup must be saved.

1.4 Backup Log

A daily backup log is issued to keep record of backups, their status, which tapes are used and housekeeping of the backup system.

1.5 House-keeping of the Backup System

Cleaning tapes are used in accordance with manufacturer's instructions. LT tape drives should be cleaned if the cleaning light is illuminated. This procedure will be done as and when needed.

1.6 Managing Backup Failure

In the event of an unsuccessful backup, the staff responsible for checking the backup must immediately:

1. Note any error messages and/or Information on the backup printout/screenshot
2. Report the failure to the Administrator and the department affected
3. Follow procedures on backup failure and re-run backup
4. If failure still occurs contact the NETCB helpdesk
5. Record the failure in the backup log and any actions taken as a result.

1.7 Storage of Backup Tapes

1. The backup tapes, when removed from the tape library, are stored securely in a fire-proof safe.
2. Once a week the tapes are taken off-site and stored securely in a fire-proof safe at the Meyerton Fire Station.
3. The off-site register and on site register must be updated and signed accordingly.
4. At the same time, the tapes deposited three weeks previously at the off-site storage will be collected and returned to the on-site safe for re-use.
   - Five days of complete backup tapes stored on the on-site premises for reuse.
   - Fifteen days of complete backup tapes (past three weeks) stored off-site at the appointed secure location.

1.8 Validation of Backups / Tapes

All restoration of data to the Solar and PayDay systems are done by the Administrators of the BCX for Solar and Payday for the PayDay systems (Disk to Disk).

1.9 Management of Tapes

1. Tapes are clearly labelled and used in strict rotation to ensure even wear and immediate identification of any problems with a specific tape.

2. All data is backed up to disk on a daily basis overnight Monday to Friday and migrated from disk to tape during the day. A cycle of four complete weeks tapes are used in rotation.

3. Financial month-end backup tapes are used in a twelve month cycle. This means that a total of 12 tapes are required for this annual backup cycle.

4. Financial year-end backup tapes are kept for a period of seven years.

5. Tapes must be replaced at the first sign of deterioration. Tapes are labelled to show age and have to be replaced according to the manufacturer's recommendations

2. Novell File Server Backup

3.1 Backups (incremental and full) of all volumes on the Novell File Server are done through BackupPC, a high-performance, enterprise-grade system for backing up Linux and stored on disk.

3.2 a Backup script runs daily and backups are done to the backup server on-site.

3.3 Incremental backups are done daily from Monday to Thursday and a full backup is taken over the weekend. On average there is four full weeks of backups on the backup server and the oldest backup will be overwritten when the disk space is depleted.

3.4 The designated member of staff (IT helpdesk operator as in 7 below)must check the backup status on the system first thing each morning and report any failures to the Administrator as per daily check list.

3.5 If failure to run a successful backup cannot be solved by the Administrator, contact VPN Technologies to report the failure for rectification.

4 BAUD Backup

This system is no longer in use and the asset management is part of the Solar system.

5 CITY Solve Backup.

The Citysolve system is hosted by I@Consulting and all data and source code are backed up on a daily basis. For detail on the SLA refer to Citysolve Support and Maintenance Agreement filed with the Development and Planning Cluster. Proof attached as “Annexure 1C”. Systems is no longer in use as from 30 September 2018.

7 Duties and responsibilities of staff responsible for backups.

All the stipulated functions above in points 1 and 2 are the responsibility of the staff members tasked to do the backups:

Systems Administrator: R.Tshabangu

Technician: M Mpaka, P.J. Otto, T Twala.

SCHEDULE 2

DISASTER RECOVERY STRATEGY.

It is recorded that a Disaster recovery server (Plate Spin Forge) for Solar (mScoa), PayDay, Quidity, Terminal services, Novell and shared drives as well as cash drawer has been commissioned by the MLM and is located at the appropriate off-site venue(Fire Station CCTV room) and the connectivity to that venue is by means of fibre optic link. This server (Plate Spin Forge) is updated daily by replicating the core systems mentioned above to this server commencing at 20h00.

Depending on the severity of the disaster the systems can be ring fenced on the DR server and the users can then access the DR server to continue the processing on the DR server. It must be mentioned that the recovery point will always be the data as replicated on the previous day's replication.

To ensure that this Disaster Recovery plan and procedure will be beneficial it is absolutely imperative to ensure that backups are taken and reports are checked on a daily basis. The replication of the mentioned core systems should be checked daily and the ring fencing and testing of the said systems as replicated should be tested and signed off quarterly.

The Disaster Recovery procedure will be deemed to come into effect when;

- A system hardware failure such as a disk crash or other hardware failures occurs and is not repairable within a 24 hour period.
- A natural disaster should occur at the Council's main computer centre at the Head Office in Mitchell street.

Should a disaster occur the following procedures should be followed:

1) In the case that the data can be recovered from a backup:
   - Recover the last successful backup from the off-site storage.
   - Check the backup cycle and tape description as defined in the backup cycle to ensure that the correct tape is recovered and restore the data to the relevant database.
   - Revert back to normal processing.

2) In the case that servers /server room were damaged or destroyed revert to the procedure to ring fence the environment and continue processing by accessing the DR server(Plate Spin Forge).
   - Inform all users that the production server is not functional and the pre-configured DR connection is to be used until such time that the production server can be fixed.

Contact Persons in case of a Disaster:

MIDVAAL L.M. **Contact numbers:**

A.S.A. de Klerk	082 771 8961	Municipal Manager
T.W. Peeters	082 859 0486	Deputy Municipal Manager
P.A. Ernst	084 500 0155	IT Operations Manager
Afrika Sibeko	073 175 5607	IT Asst Director
Rebecca Tshabangu	072 157 7621	Systems Administrator
Desmond Mosiya	083 426 8050	Technical Administrator

Fire:

Hannes Steyn	082 697 0732	Chief Fire Officer
Anthony Bruno	076 306 0345	Deputy Chief Fire Officer
Fire Control Room	016 360 7500	

Vendors:

Securelink	083 274 8948 Francois de Kock	(LAN and WAN)
VPN Technologies	083 305 3854 Jaco Lange	Firewalls, ISP and routing devices
Business Connexion	082 901 2244 Kobus Ras 076 838 1882 Jenny Bierman	Virtual Servers and Solar financial system/ Cash drawer
NETCB	82 441 7782 Justin Foxcroft 83 395 5196 Cobus Burgers	Novell/Groupwise
Payday	072 605 7799 Aldo Taylor	Salary/Human resources/leave systems, Time & Attendance and Ess
Quidity	078 882 5707 / 083 415 4875 Pam Buttle	Electronic Management

SCHEDULE 3

MIDVAAL LOCAL MUNICIPALITY

IT STEERING COMMITTEE

TERMS OF REFERENCE.

Annexure 3A (Revised August 2018)

IT STEERING COMMITTEE MEMBERS

Representative of each department nominated by the HOD

IT	Paul Ernst	Pernst@midvaal.gov.za	016 360 7557
Corporate Services	Louise van Staden	Louisevs@midvaal.gov.za	016 360 7553
Financial Services	Fanie Powell	Faniep@midvaal.gov.za	016 360 7496
Human Resources	Moipone Mothebeli	Moiponem@midvaal.gov.za	016 360 7409
Development and Planning	Eugene van der Merwe Michelle Coetzee	Eugenev@midvaal.gov.za Michelle@midvaal.gov.za	016 360 7429 016 360 7426
Engineering Services	Solomon Chivhungwa	Solomonc@midvaal.gov.za	016 360 5831
Protection Services	Corne Heymans	Corneh@midvaal.gov.za	016 360 5908

ANNEXURE 3A

Terms of reference for IT Steering Committee

That it be noted that the IT Steering Committee is the body to approve the specifications for and the acquisition of IT equipment and software, copier, faxes and printers in terms of the following principles:

1.1 Standardise equipment to facilitate repairs, maintenance and compatibility.

1.2 Centralise location of copiers, printers and faxes to facilitate control and minimise abuse: Provided exceptions may be approved in deserving and motivated cases having considered practical imperatives and efficient service delivery.

1.3 Check specifications appropriate to the need (and that specifications are not excessive).

1.4 Approve purchases/leases only after considering above principles.

1.5 If purchases/leases do not meet these criteria, do not approve.

1.6 The department that submits a request or proposal to acquire any IT equipment and software, copiers, faxes and printers (whether by lease or outright purchase), may motivate such request or proposal, but is excluded from decision-making in respect of the acquisition thereof.

2. BUDGET

That the request for purchases/leases for IT equipment/Software must be submitted to the IT Steering Committee: Provided that the Department that is motivating or requesting should have budgeted for the procurement of said equipment.

3. IT PROCUREMENT

That the Supply Chain Management Officer and Administrator consolidate and present the proposed process to purchase IT equipment and software to the IT Steering Committee for approval.

IT/ WEBSITE (MISCELLANEOUS MATTERS)

1. That all users be notified on a regular basis (6 months at least) that their information must be deleted from "Share on Meyerton", as well as e-mails, where- after there will be no access to the info.

2. That IT be involved in the induction of all new employees.

3. That Human Resources put a procedure in place to test computer literacy at interviews.

4. That all employees be informed that official mails must be opened and attended to as soon as possible.

5. That a copy of all IT equipment orders be forwarded to IT department.

6. That the rule for the Municipal Manager, Heads of Department and all staff is that passwords are to be strictly changed every 30 days.

7. That no overtime before 06h00 or after 18h00 be authorized for IT officials, accept if prior arrangements were made for a legitimate reason.

8. That it be noted that for all requests for assistance from IT, a call must be logged on the E-helpdesk system and adequate and detailed information must be provided.

9. That no software and hardware be purchased or installed if not approved through the IT Steering Committee.

10. That all packages utilized by departments be reported at the next IT meeting with applicable maintenance agreements and licenses fees payable.

11. That a register be compiled of all IT equipment in the departments.

12. That broken printers not be replaced automatically and extra printers not necessarily be purchased. That network printers be utilised . Should a desktop printer be required approval for such a procurement must be given by the DMM.

13. That in future, Management Services must inform IT on a monthly basis (monthly report) of any appointments, transfers and resignations.

14. That each HOD provide the Municipal Manager with a detailed status quo report on all laptops in the department annually during July.

15. That the HOD's apply the principle in their Department to allocate copiers, faxes and printers centrally to save costs and control usage, provided that practical considerations and effective and efficient operations also be applied.

16. That the replacement of such equipment or acquisition of new equipment be considered by the IT Steering Committee before such replacement or acquisition in pursuance of the principle in (15) above.

SCHEDULE 4

MIDVAAL LOCAL MUNICIPALITY.

STANDARD OPERATING PROCEDURE FOR ACCESS TO IT. SYSTEMS AND CONTROLS.

The IT USAGE POLICY and IT ACCESS POLICY governs the access to systems and this procedure should be read in conjunction with the said policies.

All new and existing IT users requesting access to IT. Systems (Novell, Solar, PayDay, Internet etc.) must follow the procedures as described in Section 2 of the IT Access Policy attached as “Annexure 6”.

User Access Report

1. The Systems Administrator has to generate a Solar User Access Report (ZA350), PayDay user access report and a NOVELL list of users every 45’th day of the quarter.

2. The Solar User Access Report and NOVELL list of users must be verified and signed off by the CFO and the Directors in the finance Department and all H.O.D’s. The PayDay user access report must be verified and signed off by Asst. Director Expenditure/Pay Office

3. The Administrator has to delete access no longer authorised as indicated on the ZA350, Novell / Groupwise and Payday user access reports.

Monitoring of the Administrator Activities

1. The Auditor General requested for Administrator activities to be monitored on an application and database level by an independent person.

2. The Administrator has to generate the report (ZA 380) for Solar and an administrators report must be provided by Asst. Director Expenditure/Pay Office on a monthly basis and must be included in the Proof of evidence file to be submitted to the Internal Auditors on the 15’th day of the month following the month to be audited.

SCHEDULE 5

MIDVAAL LOCAL MUNICIPALITY IT. FUNCTIONS.

Attached is the list of IT functions performed by the IT department.

1. Systems and network maintenance.
2. Anti-virus and Firewall monitoring and administration
3. Housekeeping of file servers
4. E-mail and Internet monitoring and administration
5. Radio links monitoring and maintenance
6. Maintenance of IT Infrastructure
7. Network switches setup(creation of Vlan's)
8. Setup of hardware & software
9. Network Administration and access control to systems
10. Executing Backup's and storing backups offsite
11. Execution of Disaster Recovery testing quarterly
12. UPS/Generator monitoring and testing quarterly
13. Helpdesk – allocating of logged calls to technicians, first line service to users
14. Execution of Disaster Recovery testing quarterly
15. Technical Assistance to users
16. Software Administration
17. Sourcing of IT related quotations and procurement thereof
19. IT asset verification

These functions must be reviewed by the department at least annually to determine whether anything has changed.

Reviewed August 2018 and is still relevant and accurate.

SCHEDULE 6

The following policies governs the IT procedures and needs to be reviewed annually:

IT Usage
Policy; IT
Access Policy,
IT Security
policy;
IT Change management
policy; IT Laptop policy and
MLM Master systems plan.

Copies of the policies and master systems plan attached below for approval.