Part C - Appendices

Table of contents

Appendix C12.5 – Laboratory Devices and drivers 256
Appendix C14 – Existing state..... 256
Appendix C14.8 – Right of choice..... 257
Appendix C17.11 – Reports 258
Appendix C28.6 – Backup and Restoration..... **שגיאה! הסימניה אינה מוגדרת.**

Appendix C 12.5 – Laboratory devices and drivers

See Excel file “Appendix C12.5 laboratory devices and drivers”.

Appendix C14 - Existing state

See separate file “Appendix C14 Existing state”.

Appendix C14.8 – Right of choice

1. Pursuant to Section 3C(A) of the Mandatory Tenders Regulations 5753-1993 and subject to the approval of the Division's Tenders Committee, the Division is allowed to exercise the options set forth in this appendix within the Tender.
2. The prices for exercising the options are included in the price offered by the supplier – for all elements defined as part of the required solution and priced in the tender documents. For components that are not defined as part of the required solution, the supplier will quote an exercise price if and when requested to do so. And the final price will be determined consensually between the two parties.
3. The Division will be able at its sole discretion to purchase additional elements in accordance with this appendix or issue an additional procurement proceeding, at its sole discretion.
4. The potential expansions of the tender include inter alia the following subjects (but are not limited to them):
    a. Addition of laboratories at a medical center up to 30% each year
    b. Addition of medical centers and their branches up to 15% each year
    c. Addition of hours for modifications and improvements, up to 100% each year.
    In the first year as set forth in Section 30.2.7.3 (part C).
    d. Additions for development of drivers and installations according to the requirement of the Division up to 100% each year.
    In the first year as set forth in 30.2.8 (part C).
5. Future technologies
    a. Adding a product or service as a result of technological changes
        1) In any case of technological changes that have an effect on the services provided according to this tender, the Division is allowed to request from the supplier a new product or new service or update of an existing service, based on the new technology.
        2) For examining the new technology for the purposes of the Division and adapting it to the services provided according to the tender, the Division is allowed to order from the supplier demonstrations, pilots, test environments, etc., and expert hours, from a bank of consultation hours existing in the tender.

3) A procedure for adding or updating a service will be as follows:
   - At the request of the Division, the supplier will submit a price quotation for the new product or new service or the updated service. The Division, at its sole discretion, is allowed to let the supplier subcontract for submitting the bid.
   - The Division will choose an independent advisor whose function will be to evaluate the service. To this end, the advisor will examine the bid in financial, technological and in any other respects that may provide the Ministry the best tools to decide whether the bid meets the needs of the Division, and the services provided under the tender.
   - If the supplier does not forward a bid or its bid is not approved by the advisor, the Division will be allowed to request additional bids from other bidders. The supplier undertakes to cooperate with any other bidder that will be chosen by the Division to provide the new service or updated service.
4) In any case of adding a new product or new service or updating an existing service, the Division is allowed to add to the service level agreement (SLA) additional requirements, in accordance with the character and nature of the new or updated service.
5) If the Division has chosen to extend the engagement period, in accordance with the contract (appendix 0.8.2 to the tender), the extension of the engagement will also include the new product or the new or updated service.
6) It is clarified that adding medical instrumentation for which the supplier already has an interface will be managed as set forth in Section 24.13 of the tender.

Appendix C17.11 – Reports

Barzilai Medical center

The blood bank
Name of the report
High transfusion subjects
General samples
Dispensed units
Summary of treatments for products
Tests
Daily samples log

Recently used reports
Name of the report
Work statistics
Laboratory test results report
Subject results and antibodies
Work list report - samples
Transfusion Reaction Report
Performance times (pathology - statistical)
Positive answers report
Tests by subjects
General samples
Instruments statistics
Subjects needing special units-1
Statistics report - summary
Pathology secretariat report
Statistical results report
Results Summary
Dispensed units
Pathology
Pathology

Pathology orders report
Pathology performance report
Performance times
General reports / general statistics generator

Microbiology and molecular diagnosis
Name of the report
Microbiology reports generator
General reports generator - statistical results report
General reports generator - work statistics
General reports generator - ordered tests
General reports generator - ordered tests for sending party
General reports generator - summary of activity for instrument

Rambam Medical Center

Laboratory	Name of the report
Urgent	**Disqualifications report**
	Performance times
	Work statistics
	General statistics
	Passing of laboratory tests results
	Irregular results- telephone reporting
Hematology	**Ad-hoc queries**
	General statistics
	Laboratory logs report No. 1
	Performance times.

	Disqualifications
	Results report
	Statistics
	Statistics
	Review
	Customer service
	Harmonization
Chemistry	**Laboratory test results report,** **Ranges report,** **Comments report,** **Distribution of tests by sending party**
	Telephone announcements by sending party report **Disqualifications for samples / tests report,** **Performance times.** **Telephone announcements by order,**
	Performance times report, telephone announcements report
	Work statistics report, concentrated test results report, general statistics report
	Results concentrated by sending party report **,** concentrated of results
	Statistics report
	Results report
The Laboratories Division	**Statistics report**
	Results report
Endocrinology	**Reports - quality control - disqualifications**
	Review - performance times
	Customer service - telephone messages
	Process - work list
	Process - work list - results
	Work statistics report
	Encouragement fee

	Laboratory test results report
	Samples underway report
	Results report
	Results report
	Performance times
	General statistics report
Toxicology	Disqualifications report Performance times General statistics by various profiles (sender, test, etc.) Concentrated test results for a subject or ordering party - including comments and units Telephone announcements report
	Work statistics report, concentrated test results report, general statistics report
Microbiology	**Subject results** **Microbiology reports generator** **For reporting resistant bacteria to the MoH**
	Performance times

Recommendation for Backup Policy and Methodology

Medical Centers

Date: **5.7 2023**

Version **5.0**

:

Table of contents:

1. General 265
2. Backup scheduling 266
3. Connection and linking to storage systems 266
4. Methods and recommendation for information backup 266
5. Keeping of backups (retention) 268
6. Reports and review 269
7. Backup of databases 269
8. Backup on AWS cloud 272

1. General

The term data backup refers to an action of copying information so that these copies may be used to restore the original information after an event of the information being lost. These copies are called backups. Backups are useful primarily in two cases: to restore a computer to being operable again after a disaster (disaster recovery) and for restoring a number of specific files after they have been deleted or corrupted.
Every backup strategy begins with the principle of backing up the information. The data that is backed up must be stored in some place and must be organized to a certain extent.

Goals:

Recovery Point Objective - RPO

The point in time that the restored system will reflect. The ideal state is for the RPO to be at the exact moment preceding the loss of information event. By making backups at a greater frequency, the ideal state may be approached.

Recovery Time Objective - RTO

The time that passes between the disaster and the restoration of the information and return to normal activity.

Data security

In addition to providing access to information by the information owner, unauthorized access to information must be restricted. A backup must be done in such a manner as not to endanger the information, which may be achieved by encrypting the information and correct handling of the media on which the backup is stored.

2. Backup scheduling

The backups will be done at nighttime and on weekends, because the backup burdens the access to the disks and slows down the work rate.

3. Connection and linking to storage systems

According to the recommendations of the manufacturer, it is recommended to connect to the storage systems using the fastest connection methods and protocols existing, in order to get high performance in backup with a minimum of disturbance to and noise on the network.
NAS - connection by NDMP
SAN connection by ISCSI / fiber channel

4. Methods and recommendation for information backup

Full + Incrementals
The main purpose of using this type of information backup is allowing for storage of multiple copies of the information being backed up. At the first stage, a full backup of the information is done, after which incremental backup is done – only files that have been modified since the last backup will be backed up. Restoration of a whole system to a certain point in time requires finding the last full backup made before the desired point in time and all incremental backups made since then up to the desired point in time. This backup type ensures a high level of confidence that the information required may be restored, but its disadvantage is the long restoration process and the high storage requirement.

Full + Differential
This type of information backup differs from the previous type insofar as Full + Incrementals backup backs up the increments since the last incrementals backup whereas the Full + Differential backup type backs up the changes since the last full backup, although most

backed up information may be identical to the information backed up in the last changes backup. The advantage in this information backup is that the information restoration requires only the last full restoration followed by the last changes restoration (even if there are many change backups between them).

Backup type	**Full backup**		**Incremental backup**		**Annual backup**			
Frequency	**Keeping time**	**Performance days**	**Frequency**	**Keeping time**	**Performance days**	**Frequency**	**Keeping time**	**Performance days**
Once a week	6 months	Thu, Sat	Once a day	45 days	Sun-Thu	Twice a year:	Two years	The day after half the year

Methods for using the backed-up information

Usually, using and modifying the backed up information is beneficial for increasing the backup process efficiency. These changes can improve the backup speed, restoration time, information security and use of media.

Compression

There are various methods to compress the information that must be backed up to use less storage volume.

De-duplication

When many similar systems are backed up to the same storage device, there is a possibility of great information duplication. For example, if 20 workstations operating with a Windows operating system are backed up to the same server, a major proportion of the operating

system will be backed up 20 times. The only thing required is a single backup of the common part so that the information may be restored from it to all 20 stations.

Encryption

A portable storage medium, such as a magnetic tape, poses an information security risk if lost or stolen. Encrypting the information may reduce the risk, but this process requires significant resources from the computer, so the backup speed will slow down.

Staging

Sometimes it is necessary to back up the information to an interim disk and only then copy it from the interim disk to the magnetic tape. This process may solve the problem of matching of speeds between the system being backed up and the backup storage device, as happens sometimes when backing up a computer network.

5. Keeping of backups (retention)

Daily backups (once a day, Sun-Thu) are saved for 45 days.
Weekly backups (Once a week) are saved for 6 months.
Annual backups (once every six months) are saved for two years.
In other words, if a file changes every day, the system serves 30 daily versions of it (from the last 6 weeks), approximately 25 weekly versions of it (from the last half year) and 4 semiannual versions of it (from the last two years).
It is necessary to send copies of a full backup (once a month) for keeping in an underground vault in a remote site (offsite backup).

How can we know whether the backup is successful?

When 2 consecutive backups of the same type (full or incremental) fail, a rule must be defined to send an email to the backup supervisor and the center's operation / control center.

6. Reports and review

At the beginning of the month, a rule must be defined to send an email to the backup supervisor and the center's operation / control center.

Links to the monthly reports on the backups of the previous month and the current month.

It is recommended to go over the reports to make sure that the backups work as required.

7. Backup of databases

When backing up databases, it must be made sure that the backup is consistent and according to the directions of the software supplier. If special software is being used to perform the backups, the directions of the backup software supplier on backing up Oracle and MSSQL databases must be checked. In some programs there is an option for special compatibility with the backed-up database.

Databases state with a serial number each change (deletion, update, creation of new objects) that occurs in the database (for example change 1001, 1002, etc.). The changes are recorded in a in a changes log on the one hand and are made in the computer memory on the other but are transferred to the database files afterward. The meaning of this is that when database files are copied, some of the changes have been recorded in the files and some have not been recorded yet. Therefore, when attempting to open a database that has been copied during activity, an error message occurs. This is because the database engine is not able to complete changes that have not been recorded into the files. In effect, in this state it is not possible to restore a database.

Backing up databases should be done in a manner that will allow for uniformity in the database files along with backing up the change log files. A cold backup of the database may be done when it is closed – or a hot backup when it is open, and then the standard mechanisms of each of the software suppliers as described below may be used.

MSSQL

Backup

The databases will be set up in a full recovery model for full backups and log backups – if the backups are created locally, their transfer to external media must be ensured.

It is desirable to make sure of full daily backup – this may vary according to the volume of the database and the activity load.
The frequency of backup up the log directly affects the restoration ability and the possibility of information loss (RPO) – the ideal frequency is 15-60 minutes.
Making a backup of a log is essential for the regular functioning of the system – a delay in performing a log backup may cause the system to stop.
It is recommended to perform an automatic functional check – restore verify only – when the backup is created.
Some backup software suppliers use a snapshot feature – this backup freezes the IO for the file system and must be scheduled as necessary. It is important to note that in terms of MSSQL, the snapshot allows for restoration to the point at which it was taken and not beyond – i.e., it is not possible to restore additional logs beyond this point (unlike an ordinary MSSQL backup).

ORACLE

Backup - hot backup options using Oracle:

Databases will be defined with an archive log.
Users of Oracle RMAN software that takes into account changes and creates a uniform backup. This software only backs up full areas in files and omits empty areas, making the backup volume smaller than the database size. At the end of the backup, all changes are recorded so that the backup is correct as of the time of finishing the backup.
Use of a start and end of backup command – this start of backup command orders the writing of all changes existing into the database files and orders the database to write the new changes from now on only to the change files and the memory. At the end of the backup, the end of backup command implements the changes made since the start of backup command from the change files and memory and reverts to normal mode. After the start of backup order, all files may be copied and a snapshot taken at the storage level. This backup is correct as of the time of starting the backup.
In addition, the change files (called archives in Oracle) must be backup up at as high a frequency as possible according to the required RPO. Usually after the backup a stage of deleting old archives must be added.
A delay in deleting the archives may cause the system to stop.

Most backup programs support performing a hot backup matched to the Oracle database:

Backing up by RMAN - based on our experience, in most programs, using RMAN creates a range of problems in backup and restoration alike, and is therefore generally not recommended. In addition, these programs usually create a backup only of the database without an operating system and director structure, meaning that the computer must be

backed up in addition to RMAN backup, meaning that the load on the server is double, and the restoration time is double too. Usually there will be options for backup and deletion of archives in addition to the database with separate scheduling but under the same task in the backup software.
Automatic Oracle matched backup - in VEEAM version 11, there is an ability to transfer to commands to begin / end the backup automatically and the task may include scheduled backup of archives including deletion. This is the best option based on our experience. At restoration time, it is possible through one action to get a uniform database that is correct for the backup start time. In addition, if necessary, it is possible to transfer to the computer archives that were backed up after the start of the backup, to complete the information for the last archive backup time.
Oracle matched backup through Scripts – some backup programs have an option of adding scripts before and after making a snapshot, using which we can transfer the start and end of backup commands to Oracle. In this configuration an additional backup task will be required for backing up the archive files.

Cold backup

Cold backup may be done when the database is closed – commands may be transferred to close it using scripts. During cold backup, the database is unavailable to users. In addition, closing the database will lead to low performance after restarting it. This method is less recommended - it may be used primarily before a significant system upgrade.
Cold backup of a local hot backup - performing a hot backup on the local disk (using commands and copying or RMAN) that is backed up by the computer backup to a separate medium. In the case of such a backup, it will take time to copy between drives / directories after restoring the entire computer and completing the changes from the archive files. Besides the longer restoration time, there may be states in which the external backup will be done during the internal backup, meaning that there will be no backup at all, so this option is not recommended.

Restoration (applies both to Oracle and MSSQL)

It is desirable to prepare a restoration plan for a database and the full server.
According to the plan, it is recommended to conduct a periodical check - every three months database restoration, every six months full server restoration.
When restoring a database, it is also necessary to check restoration ability to a certain point in time using the lock backups. For performing the test, it is necessary to prepare a machine with appropriate database software.

After full restoration of the machine, it must be ensured that the system is active - all databases are available, and it is also desirable to connect an application for end to end operability testing.

HANA

Log mode will be defined as Normal.
Backup will be defined using backint for the relevant backup tool at the hospital.
In the cloud, backint will be set for the relevant backup tool or for S3 in the case of AWS
The backups policy and the frequency of backup will be defined according to the policy established above and will be managed in HANA Cockpit
Snapshots - if snapshots are taken of the HANA server, it is necessary not to back up the log disk.

8. Backup on AWS cloud

To define a backup process using AWS (Amazon Web Services), the following general stages must be performed:

1. Identification of the data and resources that must be backed up: which data and resources in the AWS environment must be backed up. This may include databases, file systems, virtual machines or other data types.

2. Select suitable backup service: AWS provides a number of backup services, each with its own characteristics and use cases. A number of popular options include AWS backup, Amazon 3S versions, screenshots of Amazon EBS and automatic backups by Amazon RDS. Select the service best matching your requirements.

3. Setting a backup schedule according to the policy set above.

5. Tracking and checking of backups: regularly track your backups to make sure that they run successfully, and that the data is stored securely. Also, it is important to check the restoration process from time to time to make sure that backups may be restored when necessary.

6. Automation of backup processes: to the extent possible, automation of the backup process to ensure consistency and minimize human errors. AWS provides tools such as AWS CLI, AWS CloudFormation and AWS SDKs to help you make the backup processes automatic.

It is recommended for the automation to be done at the organization level rather than at the account level or specific resource level.

7. Implementation of security measures: apply suitable security measures to protect your backup data. This may include encryption, access controls and ordinary security controls.

8. Documentation and update of backup procedures: documentation of the backup procedures and all relevant configurations. The documentation must be saved updated when changes are made in infrastructure or backup policy.

9. The backup strategy must be regularly reviewed and optimized: the backup strategy must be reviewed to make sure that it corresponds with evolving business requirements.

The backup process must be optimized to reduce costs, improve efficiency and deal with any possible weak points.

The specific changes may change according to the AWS services chosen and the character of the data.

It is always recommended to read the official AWS documentation for the specific services that are used to ensure that you work according to the most current methods and directions.