Service Level Agreement

Weather Data Application

Opdracht: *Leertaak 4 (SLM2), thema 2.1-I, groep 1*

Auteurs: *Tom Broenink, Ward Holthof, Yuri Hoogeweg,*
André Nanninga en Maurits van Mastrigt

Datum: *25 juni 2014*

Table of Contents

- 1 General **3**
  - 1.1 Definitions 3
  - 1.2 Parties 3
  - 1.3 Introduction 3
  - 1.4 Approval SLA 3
  - 1.5 Service description 3
  - 1.6 Service Continuity 4
  - 1.7 Priority Definitions 4
  - 1.8 Responsibilities 5
- 2 Customer Services **6**
  - 2.1 Weather Data Application 6
  - 2.2 Service desk 12
- 3 Pricing **15**
  - 3.1 Implementation Costs 15
  - 3.2 Structural Costs 15
  - 3.3 Service desk support 15
  - 3.4 Service Level Packages 16
- 4 Implementation & Conditions **18**
  - 4.1 Demands to Infrastructure 18
  - 4.2 Estimated Date of Delivery 18
  - 4.3 Trial period 19
  - 4.4 Bonus & Malus 19
- 5 Reporting **20**
  - 5.1 Service Review 20
  - 5.2 Trial Period Report 20
- 6 Glossary **21**
- 7 Signatures **22**

1 General

In this chapter you will find a general description of the service and requirements.

1.1 Definitions

These are the definitions used throughout this Service Level Agreement (SLA).

- **Application:** The weather data application. Including new versions of the software, as defined in the agreement and service description;
- **Service desk:** The point of contact for the customer for changes and problems regarding the service;
- **Service:** The service (and maintenance) that's supplied to the customer;
- **Authentication:** Electronic identification to ensure that the user trying to access the service is authorized to do so;
- **Incident:** A disturbance that keeps a user(s) from (partially) using a service;
- **Major Incident** A severe incident that cannot be solved within the MPT;
- **Problem:** A collection of incidents that might indicate a common cause;
- **Initial Responce time (IRT):** Within this time a response should be given to a new incident;
- **Maximum Process Time (MPT):** Within this time a incident should be resolved or be scaled up to a major incident / problem;

1.1.1 Weather data

One of the services in this SLA speaks about weather measurements. As there are some important measurements that are part of the service as defined here.

- **Wind speed:** Wind speed is the measure motion of the air with respect to the surface of the earth covering a unit distance over a unit time.
- **Rainfall:** The amount of rain that falls in a particular area.
- **Temperature:** The degree or intensity of heat present in a substance or object, especially as expressed according to a comparative scale and shown by a thermometer or perceived by touch.
- **Humidity:** Humidity is the amount of water vapor in the air. Water vapor is the gaseous state of water and is invisible.

1.2 Parties

This Service Level Agreement (hereafter called: SLA) is a contract between the following parties:

- **Client:** Aleksandro Stulginskio Universitetas - Faculty of Water and Land Management;
- **Supplier:** United Nations Weather Data Management Institute - Da Vinci Data;
- **UNWDMI:** The United Nations Weather Data Management Institute, the umbrella organisation of Da Vinci Data
- **Users:** The students and teachers of Aleksandro Stulginskio Universitetas;

1.3 Introduction

This Service Level Agreement (SLA) applies to all by Da Vinci Data signed contracts between Da Vinci Data and the client. This SLA describes the scope and the general requirements of the service to be delivered by Da Vinci Data.

On initial delivery of the service, Da Vinci Data and the client will sign a service contract. This service contract describes what the requirements are under which the service will be supplied to the client. This contract can be altered by the supplier; changes in the contract will therefore prevail above the definitions in this SLA.

The percentages and goals in this SLA are based on the 'gold' service level. The differences between levels are defined in the paragraph *3.4 Service Level Packages*.

1.4 Approval Service Level Agreement

The approval of the SLA is a shared responsibility between the supplier and the client. If the SLA has to be altered, the responsibility for changing the SLA lies with the supplier. Permission for changes has to be given by the supplier. When changes have been made in the current SLA and the aspects of the service, the new SLA has to be agreed on by the supplier as well as the client.

1.5 Service Description/Definition

The client wants to perform calculations on weather data to conduct research on climate change. The client is interested in climate change in Lithuania and other countries around the Baltic Sea and is especially interested in weather changes regarding the milder weather in the past years.

The client is interested in the following measurements:

- Wind speed
- Rainfall
- Temperature
- Humidity

The relevant countries:

- Lithuania
- Denmark
- Germany
- Poland
- Kalingrad (Russia)
- Estonia
- Latvia
- Finland
- Sweden

1.5.1 Application

The client wants a SSL secured webpages protected by a username and password showing a map of the Baltic countries. When clicking on a weather station the client wants a 'cockpit'-like view showing the wind speed, rainfall, temperature and humidity (color coded) per minute.

The application should have historic data of days, weeks and months included. Data should be saved for at least a half year. Allow this data to be downloaded.

1.5.2 Queries

The client wants to see data visualised according to the following two 'queries':

1. Rainfall above 10 mm within 50 km.
Show data about rainfall when the rainfall is more than 10 mm. Don't show when rainfall is below that.
This query only applies to weatherstations within 50 km of the coastline of the Baltic Sea.

2. Graphs of temperature and humidity.
Be able to show a graph of temperature and humidity of any individual weatherstation (since previous mid-night).
This query applies to any weatherstation worldwide.

1.5.3 Client's requirements

The client's requirements regarding the service are:

- 'Cockpit'-like graphical representation;
- History of data by days, weeks & months;
- Data retention: 6 months;
- Support for Google Chrome & latest version of Internet Explorer;
- Data & webinterface will be hosted by Supplier;
- Map with colourcode for windspeed and temperature values;
- Authenticate using username and password;
- No specific user roles, all users get the same permissions.
- Allow for data (for the past half a year in days/weeks/months) to be downloaded in Excel file;
- Only measurements per minute;
- SSL to secure safe datatransport.

1.5.4 Responsibilities supplier

Supplier will make sure the service will satisfy the following requirements:

- The service will be up 24/7, but the different queries have different availability requirements;
- Data will be backed up in different intervals depending on the query;
- There are different maximum response times defined depending on the query;
- Supplier will deliver monthly service reports;
- Supplier will set up a service desk;
- Supplier will ensure access is possible for 50 users.

1.6 Continuity of the service

To preserve the continuity of the service, all software and data will regularly be backed up. Additional information on ways of preserving the continuity can be found in chapter 2.1.1 Service Levels under the sub-heading *'Security'*.

1.7 Priority definitions

The following priority matrix will be used to define the IRT and the MPT.

1.7.1 Urgency definition

The urgency level defining the impact on the working process:

Urgency	Level
Service is not hindered	Low
Service is hindered	Medium
Service has stopped	High

1.7.2 Impact definition

The impact level defined by the amount of users affected:

Users affected	Impact level
The incident affects one user	Low
The incident affects several users	Medium
The incident affects a majority of users	High

1.7.3 Priorities Table

This matrix defines the priority of an incident, depending on the impact and urgency.

Impact / Urgency			
Impact High	High	Medium	Medium
Impact Medium	Medium	Medium	Low
Impact Low	Medium	Low	Low
	Urgency High	*Urgency Medium*	*Urgency Low*

1.8 Responsibilities

Da Vinci Data is under no circumstances responsible if the requirements in this SLA are not met, if either:

- The cause of the requirements not being met was out of Da Vinci Data's Control, such as:
  - Earthquakes
  - Fire
  - Theft
  - Floods
  - Epidecimics
  - Wars
- If the incident has not been caused by Da Vinci Data, but by the client or a third party.

2 Customer Services

In this chapter you will find a description of the Customer services (Weather data application and Service desk).

2.1 Weather data application

The client wants to perform calculations on weather data to conduct research on climate change. The client is interested in climate change in Lithuania and other countries around the Baltic Sea and is especially interested in weather changes regarding the milder weather in the past years.
Da Vinci Data provides an application that allows the client to access the weather data.

The application will be used by 50 users who will all need a username and password in order to use the application. The service will be made available using an SSL connection. The application will be hosted in the Netherlands using a server that is property of the UNWMDI.

The supplier offers the following features in the application:

- A way for the customer to get a representation in which the rainfall of each weatherstation within 50 km of the coastline around the baltic sea is shown. (if the rainfall was more than 10 mm)
- A way for the customer to get a representation in which the temperature and humidity since the most recent midnight of any UNWDMI weather station is shown.
- A map showing weather stations with a colour code depending on the current temperature.
- A way for the customer to download data of the last 6 months in an Excel (files contain either a day, a week or a month of information)

These features offer an intuitive and cockpit-like feeling to the application, enabling users to easily access detailed information on current weather data as well as weather data from any period in the last 6 months.

The supplier manages to the following facilities needed to provide the service:

- A webserver containing the application;
- Certificates needed to make the SSL connection possible;
- The nessesary technical infrastructure (Computers, Firewalls, Routers, Kabels, etc.);
- Other infrasturcture, e.g., physical space, power supplies, offices, etc.;

These facilities offer users the possibility to access the service using the internet.

To support the development and implementation as well as continued operation of the service, Da Vinci Data offers the following services:

- System administrators, application administrators, maintanance of the service;
- Services needed to implement the service, e.g.:

  - Project management
  - Preparatory research
  - Functional an technical design
  - Software Programming
  - Testing
  - Installation
  - Education
  - User management

- Operational support, i.e. First- and seccond level service desk support;
- Installation of hardware and software at the client, if nessesary;

2.1.1 Service Levels

This chapter will describe the service levels regarding the weather data application. This chapter was written assuming no particular Service Level Package. The chapter *Service Levels* contains more information on the options and differences between these options.

Availability

The weather data application has a minimum availability of 99.5% on Mondays before 12:00. However, because this is a web application, the supplier will strive to keep the application available even outside of peak times. However, the supplier can not guarantee an availability percentage over this time period. The supplier will strive to perform all maintenance related processes during this time.

Because the initial requirement was for the weather data application to be accessible on Mondays before 12:00, this will now be deemed the peak times of the service. Depending on the service level, the supplier offers a higher minimum availability during these peak periods. (minimum of 99.5%)

Service Level Targets

Several Critical Success Factors (CSFs) and Key Performance Indicators (KPIs) have been outlined to define the Service Level Targets in a clear and concise manner.

Service Level Targets of the weather data application can be summarized in the following way;

Query load time

Both queries have a maximum load time of 1 minute on Mondays before 12:00. Only authorised users will be able to issue a query request.

N.B.: the supplier guarantees the maximum load time of 1 minute only when there is no problem on the customer's side slowing the load time down. Chapter *1.8 Responsibilities* contains more information on situations like these.

Critical Success Factors

The following points are of utmost importance in successfully keeping the weather data application available and ensuring it meets the Service Level Targets.

- Data must be retained for at least 6 months and available 99.5% of the time on mondays before 12:00
- Graphs/Maps related to the queries must load within 1 minute.
- Data must be backed up starting from every midnight (until the next midnight).
- The data may not be viewed or accessed by third parties.

Key Performance Indicators

The metrics below have been defined from the Critical Success Factors, these metrics will be used to measure the quality of the services.

Data must be retained for at least 6 months and available 99.5% of the time on mondays before 12:00

Metric	Goal	Source
Uptime service	98%	Measured uptime service.
Uptime service during opening times	99.5%	Measured uptime service.
Uptime service during peak hours	99.5%	Measured uptime service.

Graphs/Maps related to the queries must load within 1 minute.

Metric	Goal	Source
Average response time	< 1 minute	Response time measured in tests on a wide variety of systems.
Maximum response time	< 1 minute	Response time measured in tests on a wide variety of systems.

Data must be backed up starting from every midnight (until the next midnight).

Metric	Goal	Source
Amount of failed or incomplete backups	0	Amount of incidents involving a corrupt or missing backup.

The data may not be viewed or accessed by third parties.

Metric	Goal	Source
Amount of security breaches compromising data	0	Amount of security related incidents involving (suspected) successful retrieving of information by third party.

Losstime

To ensure service availability and data integrity, the supplier set up a maximum losstime. The definition of losstime is the amount of hours it takes for a backup to be restored after an integrity incident. This inevitably means that some amount of data depending on the losstime will be lost.

The maximum losstime for weather data is half an hour. If this loss time is exceeded, the supplier will schedule a service review with the client to evaluate why the loss time was exceeded and what measures can be taken to prevent this from happening.

Maintenance

Service maintenance will take place during set times. This will be on tuesday nights between 19:00 and 21:00 (if necessary). When maintenance has to urgently be performed (because the continuity or integrity of the service may be at risk), this will take place in accordance with the client. Customers will receive notice of maintenance at least half an hour before the start of the maintenance.

The duration of maintenance may depend on the severity of the issues and the uptime guarantee depending on the service level package.

Calculation:

A year has 365,25 (0,25 days to account for leap years). The peak time (Mondays before 12:00) accounts for 12 hours a week. Which is 12 / 7 = 1,71 hours a day on average. Or 1,71 * 365,25 = 626,14 hours a year on average. And 626,14 / 24 = 26,09 days a year on average.

Time	Days	Hours	Availability	Maximum hours of downtime yearly
Peak times	26,09	626,14	99.5%	626,14 * 0,03 = **18,78**

The maximum amount of downtime a week during peak times is 26,09 / 52 = 0,50 hours (30 minutes).

Expected maximum amount of problems a year.

The supplier expects to encounter no more than 150 problems a year. Problems are defined as: anything that is not out of the supplier's control that will negatively impact the availability of the service for one or multiple users during the peak times.

Security

Because the information is of great value to the supplier as well as the client, both these parties will take security measures to ensure the data remains secure. These security measures will be outlined and described in this chapter.
The supplier will setup a SSL-connection to secure safe data transport. Users of the application will agree to not store usernames or password locally. There will be a total of 50 users, with no segregation in privileges.

Backups

An incremental backup of all data used in the service will be started at midnight (local time in Kaunas) on every day and kept until the next midnight. This ensures that the client will always have access to the most recent data.

After an integrity incident, the daily backup will prevent data loss for the most part. The maximum amount of lost data will be equal to the amount of downtime. The supplier estimates that restoring a backup will not take more than an hour.

Password policy

To prevent third parties from gaining access to the system by exploiting weak passwords, the service will enforce a password policy for all users. The password policy consists of the following requirements:

- Users are obliged to change their password every two months, before the first Monday of the month.
- Passwords have to meet the following requirements:
    - At least 8 characters
    - At least 1 capital letter
    - At least 1 symbol

Of course the passwords will be saved in a secure way (hashed and encrypted).

Customer responsibilities

Even secure, complex passwords can be compromised. It is for this reason that the supplier also places strict requirements on the security on the customer's end.

Every customer logging in to the service needs to:

- Have ran a virus scan in the past week.
- Immediately change his/her password and notify the service desk if the customer suspects a third party has gained access to his/her account.

Monitoring

All software-related incidents will be logged. These logs will be saved. There are a couple conditions to this process:

- Logs will be saved up until a month after the incident.
- Depending on the priority of the incident, the supplier may decide to keep the log permanently. Especially if the supplier suspects this incident may indicate a problem in the future.

Calamities

The supplier defines calamities as incidents such as:

- Power outage
- Fire
- Theft

In the unlikely event of a calamity, the supplier will take immediate action to attempt to get the service back up and running as soon as possible. The supplier estimates that the service will always be back up within 5 hours of the event happening.

The *Responsibilities* paragraph contains more information on what a calamity is and when a calamity is deemed 'beyond the supplier's control'.

The paragraph *Backups* states that backups will be kept on a regular basis. These backups can be used in the event of a calamity to ensure the service will be back online with the least amount of data loss possible.

2.1.2 Risk Analysis

This chapter describes the possible risks for the availability of the application, and included are the measures to possibly prevent the risks.

Risk descriptions

The following table shows our risks and measures:

Risk	Chance	Impact	Measure 1	Measure 2
Internet outage	low	low	Backup internet connection	Contracts with reliable parties
DDoS attack on data center	low	High	DDoS protection software	Intervention plan DDoS
Server software failure	Medium	High	Maintenance contract with supplier	Employees with sufficient expertise
Server harddrive failure	Medium	Medium	Raid configuration	Monthly S.M.A.R.T./drive tests

2.1.3 Capacity planning

The Weather Data Application is expected to cause the most workload on the storage space of the server. The supplier does not expect the graphical representations and the calculations needed for these to cause too much strain on the system itself. However, the application might cause some strain on the storage space, seeing as all data has to be saved over a period of 6 months. Because the supplier has not yet processed 6 months of data it is hard to make an exact measurement concerning the maximum amount of storage space needed.

Instead of an exact measurement, the supplier has made a rough estimate, assuming that the amount of data per day will stay consistent and not taking into account caching/compression algorithms that may be implemented at a later stage:

As seen in the calculation, a maximum amount of storage space of *GB* will be required to store half a year of weather data.

To ensure that the application will not run out of storage capacity, the supplier will strive to maintain an overcapacity of 10%. Important to note is the ease of adding additional storage space. The expectation is that the supplier will be able to provide the application with additional storage hardware at any given moment (given the necessary hardware is available on site), this process will not cause more than 30 minutes of downtime.

The total startcapacity including the overcapacity margin for the Weather Data Application will be: ** 1,10 =*

2.2 Service desk

The supplier will support the weather data application with a Service desk. The Service desk will be hosted in the Netherlands and will be available for all users of the application. The Service desk will be available from Monday to Friday from 07:00 to 20:00 (local time in Kaunas). Employees of the service desk will be English speaking.

Users can contact the service desk for:

- Questions and advice about the application and its functionality;

- Recording, analysing and resolving of incidents;

2.2.1 Service Levels

Availability

The service desk will be available from Monday to Friday from 07:00 to 20:00 (local time in Kaunas). Minimal availability between these hours will be 97%.

Below you will find the Critical Success Factors and Key Performance Indicators that belong to the Service Level Targets.

Critical Success Factors

The following points are critical for the success of the service desk:

- Responding to new incidents on time.
- Resolving new incidents on time.
- The availability of the service desk.

Key Performance Indicators

Below you will find the standards that define the Critical Success Factors. These will be used to measure the quality of the service.

Timely response to new incidents.

Measurement	Goal	Source
Amount of incidents with exeeding IRT	< 15	Amount of incidents without response within the agreed upon IRT from the last 3 months.
Average IRT of incidents with high priority.	< 15 minutes	Average IRT of all solved incidents with high priority from last 3 months.
Average IRT of incidents with medium priority.	< 1 hour	Average IRT of all solved incidents with medium priority from last 3 months.
Average IRT of incidents with low priority.	< 2 hours	Average IRT of all solved incidents with low priority from last 3 months.

Timely resolving of incidents.

Measurement	Goal	Source
Amount of incidents with exeeding MPT	< 15	Amount of incidents without resolution within the agreed upon MPT from the last 3 months.
Average resolve time of incidents with high priority.	< half an hour	Average resolve time of all solved incidents with high priority from last 3 months.
Average resolve time of incidents with medium priority.	< 4 hours	Average resolve time of all solved incidents with medium priority from last 3 months.
Average resolve time of incidents with low priority.	< 8 hours	Average resolve time of all solved incidents with low priority from last 3 months.

The availability of the service desk.

Measurement	Goal	Source
Amount of complaints.	0	Amount of complaints recieved by the Service Manager.

Response and process times

The maximum time spent on solving a incident depends on the priority of the incident. The maximum response- and processtime with a gold-level service desk is as following:

Priority	Initial Response Time	Maximum Process Time
High	Within 15 minutes	Within 30 minutes
Medium	Within 1 hour	Within 4 hours
Low	Within 2 hours	Within 8 hours

2.2.2 Risk Analysis

The service desk can also be subject to several risks. Although some of these risks are highly unlikely the supplier must prepare for the consequences these might propose, as the supplier wants to warrant the availability.

Risk descriptions

Risk	Chance	Impact
Phone defects	Low	Medium
Online-chat failure	Medium	Low
Email failure	Low	Low

The consequences of a phone defect is described as 'medium' because phone contact is the most efficient way of contacting the Service desk. Phone contact ensures a fast transfer of information and allows the service desk employee to
question and troubleshoot with the user.
A failure in the online-chat system has a higher probability but has no major consequences. When the online-chat function is no longer available, users will still be able to phone the Service desk.
An email failure is also very unlikely and even though this is a preferred means of communication for users, it is not a very functional way of communication. Therefore, the supplier considers the consequences to be low and gives it a low impact.

Measures

In order to saveguard the availability of the Service desk the supplier will increase the response times of these means of communication. Depending on the service level (Gold, Silver, Bronze) there will be a higher response time of the Service desk. This ensures that whenever one of the risks occurs, users can fallback to one of the other means of communication.

2.2.3 Capacity planning

Because there will be a fixed amount of users on the system, the supplier can make an accurate estimate of the amount of users that will contact the Service desk.

If at any time reports show that the Service desk cannot handle the amount of incidents, there will be an evaluation to decide if the budget for the service desk is still realistic or if some changes in this SLA need to be made in order to guarantee the Key Performance Indicators (as described in *2.3.1 Service Levels*).

If the conclusion at the end of the trial period shows that the amount of estimated incidents and problems is much higher or lower as initialy suggested, the supplier and client will redefine these estimates (as described in *4.3 Trial period*).

3 Pricing

3.1 Implementation costs

To set up the service desk to support the new weather data application, new hardware and service desk training/employees will be necessary. These processes cause implementation costs:

Part	Costs
Development wather data application	€ 10.125,-
Hardware costs weather data application (Webserver)	€ 4.900,-
Hardware costs weather data application (Database server)	€ 8.000,-
Service desk (Hardware)	€ 2.000,-
Total:	**€ 25.025,-**

After the execution of the implementation processes, changes and maintenance can cause other costs. For example, the supplier will keep maintaining the software, ensuring it is up to date and remains bug-free. The client is obliged to start using the new releases within 6 months after the supplier delivers a new release. The estimated cost for this service is **€2700,-** yearly. This includes installation, delivery, convertion and education for the service desk staff.

3.2 Structural costs

To provide continued use of the weather data application, a monthly sum will be needed for, for example, hosting. In addition to that, the service desk employees will need to be paid. Due to situations like these, the following structural costs have been defined:

Monthly	Yearly
€ 1.725,-	**€ 20.700,-**

3.3 Service desk support

The service desk will recieve a monthly sum of € 1.000,-. This money will be used for the development and maintenance of the service desk. For example:

- Keep the knowledge up-to-date when the weather data application gets a new release.

- Expand on service desk infrastructure and hardware when necessary.
- Hire new employees temporarily during release procedures.
- Licence management.

3.4 Service Level Packages

In this chapter, each the customer- and basic services' KPI's will be listed for each service level. The available service levels are bronze, silver and gold.
The numbers used in this chapter are based on amounts per month.

Weather data application

Weather data application	**Bronze**	**Silver**	**Gold**
General uptime.	95%	97%	98%
Uptime during peak times and opening times.	97%	98%	99.5%
Amount of changes available	6	9	12
General load time for queries.	< 60 seconds	< 30 seconds	< 10 seconds
Maximum amount of incidents with high priority	< 10	< 6	< 3
Maximum amount of incidents with medium priority	< 50	< 35	< 20
Maximum amount of incidents with low priority	< 100	< 75	< 50
Minimum score security report.	n.v.t.	7	9
Maximum amount of unsolved integrity incidents.	5	3	0

In the table below, the risks will be listed along with the measures that will be taken to prevent or react to these risks for each service level package.

Risk	Measure 1	Measure 2	Bronze	Silver	Gold
Server instability (hardware fault)	After trial period, deliver a report evaluating the current hardware and different options	Free periodic hardware upgrade	-	1	1 & 2
DDoS attacks	Software to prevent DDoS.	Create an intervention plan.	-	1	1 & 2
Software fault (security/stability)	Real-time bug reporting to the development and maintenance team.	Set up a dedicated bug-resolving team	-	1	1 & 2

Service desk

Service desk	Bronze	Silver	Gold
Service desk availability.	95%	97%	99%
Max. amount of incidents that are exeeding the IRT.	< 10	< 8	< 5
Max. amount of incidents that are exeeding the MPT.	< 10	< 8	< 5
IRT of the service desk - priority high.	30 minutes	20 minutes	15 minutes
IRT of the service desk - priority medium.	4 hours	2 hours	1 hour
IRT of the service desk - priority low.	6 hours	4 hours	2 hours
MPT of the service desk - priority high.	90 minutes	1 hour	30 minutes
MPT of the service desk - priority medium.	8 hours	6 hours	4 hours
MPT of the service desk - priority low.	3 working days	2 working days	8 hours
Maximum amount of service desk complaints	5	3	0

Yearly costs for each service level

Component	Bronze	Silver	Gold
Weather data application	€ 6.900,-	€ 10.350,-	€ 20.700,-
Service desk	€ 2.000,-	€ 6.000,-	€ 12.000,-
Changes and Maintenance of the application	€ 900,-	€ 1.350	€ 2.700,-
Total:	**€ 9.800,-**	**€ 17.700,-**	**€ 35.400,-**

4 Implementation and Conditions

4.1 Demands to Infrastructure

The management of the IT-services of the company should be performed professionally with a high availability. The demands mentioned in *1.5 Service Description/Definitation* can be translated to the following demands of infrastructure:

- Data and webinterface will be hosted by the Supplier;
- Application must be compatible with Google Chrome and the latest version of Internet Explorer;
- Users must authenticate using their personal username and password;
- Allow for data to be downloaded in Excel file for the past half a year in days/weeks/months;
- SSL to secure safe data transport.

4.2 Estimated date of delivery

The estimated date of delivery is 26th of June, 2014.

4.3 Trial period

This agreement has a trial period of six months. During this period, the set requirements and goals will be evaluated to determine whether they are realistic or not.

At the end of the trial period, an extra report written based on the monthly Service Level Reports will be delivered. This report will describe every service and evaluate if each individual service requirement is reachable and which service requirements may need to be adjusted. Following the delivery of the report to the client, an evaluation will take place between the client and the supplier.

There are no bonus and malus arrangements during the trial period.

4.4 Bonus and Malus

There are bonuses, fines or other penalties defined in this Service Level Agreement. When the promised requirements, as defined in chapter *1.4 Service Description* are not fully met, a warning will be issued by the client. After a warning, The supplier will start an internal evaluation and investigation to determine why they failed to deliver on the promised requirements.

When three warnings have been issued by the client, the supplier as well as the client will evaluate the situation together and possibly alter the SLA in order to guarantee meeting the requirements.

5 Reporting

5.1 Service Review

The supplier will deliver a Service Level Report to the client on a monthly basis. This report will evaluate the goals set for each Critical Success Factor and the measured values for each CSF. This offers a clear overview of the desired quality of every service and whether or not these goals were accomplished. If the Critical Success Factors have not been met, this will be elaborated on in the report. Based upon this report, the supplier can determine where and if there's room for improvement in cooperation with the client.

The Service Level Report will be delivered within 10 days after the end of the month.

The enclosure *"Example Service Level Report.pdf"* offers an example of what a Service Level Report would look like.

5.2 Trial period report

At the end of the trial period, a report will be written based on the monthly Service Level Reports. In this report, all goals and requirements, expressed in Critical Success Factors (CSF) will be elaborated on. For each CSF the feasability and set goals will be listed and evaluated.

When the supplier fails to meet a goal's requirements regularly (more than 3 months in a row), this goal can be deemed unfeasible and the goal's requirements have to be reevaluated. Goals will also have to be reevaluated if the set goal is not met by a wide margin. (for example 70% instead of 99% availability would be considered 'by a large margin')

6 Glossary

Glossary

The following list contains an explanation of the technical terms used in this SLA. They are ordered alphabetically.

- **Server**

> *A server is a computer that provides data to other computers. It may serve data to systems on a local area network (LAN) or a wide area network (WAN) over the Internet.*
> *— http://www.techterms.com/definition/server*

- **SSL Connection**

> *Stands for "Secure Sockets Layer." SSL is a secure protocol developed for sending information securely over the Internet. Many websites use SSL for secure areas of their sites, such as user account pages and online checkout. Usually, when you are asked to "log in" on a website, the resulting page is secured by SSL.*
> *— http://www.techterms.com/definition/ssl*

7 Signatures

This agreement has been made between Aleksandro Stulginskio Universitetas (client) and Da Vinci Data (the supplier) of the UNWDMI.

The agreement has been agreed on and signed on two copies, at ……., on …… / …… / …… .

Starting date of the agreement: …… / …… / ……

Signature client:

Name	Signature

Signature supplier:

Name	Signature