



SERVICE LEVEL AGREEMENT

Information Technology Systems & Services



MANAGEMENT SCIENCE ASSOCIATES, INC.

RockPointe Business Park

400 MSA Drive

Tarentum, Pennsylvania 15084-2808

TEL 724.265.6500 • FAX 724.265.5738

©2008 Management Science Associates, Inc.
All material contained within is for the internal use of MSA employees only.
Contents cannot be republished or reproduced in any form.

Table of Contents

1. INTRODUCTION.....	1
2. MSA RESPONSIBILITIES AND OBLIGATIONS	1
2.1. INSTALLATION AND CONFIGURATION	1
2.1.1. <i>Training</i>	1
2.2. SUPPORT AND PROBLEM ESCALATION	2
2.3. BACKUP AND RESTORATION OF CUSTOMER DATA.....	2
2.4. SERVICE UPGRADES AND MAINTENANCE.....	2
3. CUSTOMER RESPONSIBILITIES AND OBLIGATIONS	2
3.1. INSTALLATION AND CONFIGURATION	3
3.2. SUPPORT AND PROBLEM ESCALATION	3
3.3. CUSTOMER BACKUP AND RESTORE OF DATA.....	3
3.4. REPORTS	4
3.5. SERVICE AND MAINTENANCE.....	4
4. SUPPORT AND ESCALATION PROCEDURE.....	4
4.1. CUSTOMER ESCALATION PRIORITIES	4
4.2. DISASTER RECOVERY - HIGH PRIORITY	6
5. PERFORMANCE LEVEL AGREEMENT.....	7

1. INTRODUCTION

This document details specific responsibilities for both MSA and the Customer to ensure that the Remote Data Protection service is properly commissioned. This document defines what shall happen in the event a problem occurs. The document also specifically details those circumstances under which the service shall be deemed to be outside of the Service Level Agreement (SLA).

2. MSA RESPONSIBILITIES AND OBLIGATIONS

MSA shall provide an automated mechanism whereby the Customer shall be able to back up data from all designated servers and network connected desktop computers as defined in the Remote Data Protection Service Guide.

Subject to the conditions outlined in this document MSA shall undertake that the product and services delivered to the Customer shall function as specified.

2.1. Installation and Configuration

An MSA authorized representative shall deliver, upon execution of the Services Agreement, the specified products and services to the Customer for installation and configuration. MSA shall provide up to eight (8) hours of telephone support and/or training regarding initial configuration. All such service by provided by telephone.

Should Customer prefer, MSA may perform the installation and configuration. MSA shall coordinate with the Customer a mutually agreed upon date, time, and price. In this event, no “no cost” training shall be rendered.

2.1.1. Training

If the Customer implements its own installation and configuration, an authorized MSA representative shall provide the following training for the designated authorized Customer representative as defined in the Remote Data Protection Service Guide, if requested by Customer and subject to the above time limitations:

- Create a backup set, to administer and schedule backups, and to restore data from the Remote Data Protection System.
- Demonstrate that the service is capable of backing up data from the Customers’ network.

At the conclusion of training, the MSA authorized representative shall transfer the Remote Data Protection service to the Customer and notify the MSA Data Center that the service is live and fully commissioned. MSA Technical Support shall present the designated authorized Customer representative with a Service Report.

2.2. Support and Problem Escalation

MSA shall provide 24-hour x 7 day-a-week Customer telephone support to respond to Customer inquiries within the scope of this Agreement.

Calls shall be handled strictly in accordance with the escalation procedures outlined in the Support and Escalation Procedure section of this document with priority being given to the most severe.

2.3. Backup and Restoration of Customer Data

MSA shall be responsible for ensuring that the Remote Data Protection Service and all associated components, within the immediate control of MSA, shall be available to back up Customer data that has been defined in all valid backup sets by the Customer.

2.4. Service Upgrades and Maintenance

MSA shall be responsible for the provision, management and installation of all product and service releases and engineering changes (hardware, software or firmware) that it deems necessary to maintain and/or upgrade the product and services.

IMPORTANT: Upon installation, Customer shall be required to select encryption level and encryption keys. MSA shall accept no responsibility for storing Customer's Remote Data Protection encryption keys. Loss of the encryption keys by the Customer shall prevent recovery of the Remote Data Protection service and the Customer's backup data.

3. CUSTOMER RESPONSIBILITIES AND OBLIGATIONS

Although Remote Data Protection is a managed service proposition and MSA shall be responsible for the availability of the service components, the day-to-day operation of the Remote Data Protection service shall depend on certain key processes and related equipment which are wholly under the Customer's control.

3.1. Installation and Configuration

The Customer shall be responsible for providing authorized and free access for an MSA authorized representative to deliver the product and services to site on a pre-arranged installation date.

The Customer shall be responsible for providing the necessary power, network connection, and appropriate environment to support the DS-Client Appliance as defined in the Remote Data Protection Service Guide.

The Customer shall make available a designated and appropriately qualified representative to work with the MSA authorized representative during the installation of all the necessary product and services, as defined in the contract.

The Customer designated representative shall confirm that the backup functionality of the service has been demonstrated to his/her satisfaction.

The Customer designated representative shall then accept delivery of the Remote Data Protection Service as a fully commissioned service. The Customer designated representative shall sign the Service Report and present this to MSA Technical Support.

IMPORTANT: The Customer is solely responsible for storing their Remote Data Protection encryption keys in a secure location. Loss of the keys by the Customer shall prevent recovery of the Remote Data Protection service and the Customer's backup data.

3.2. Support and Problem Escalation

The Customer designated representative shall be responsible for promptly reporting any problems directly to MSA's Customer Support in accordance with the escalation procedures outlined in the Support and Escalation Procedure section of this document.

3.3. Customer Backup and Restore of Data

The Customer shall be responsible for the availability of their network and those systems to be backed up by the Remote Data Protection Service.

The Customer shall be responsible for defining appropriate backup sets and schedules for those systems to be backed up.

Remote Data Protection cannot guarantee to successfully back up all open files. The open files that fail to back up are reported to the Customer by

the Remote Data Protection service. The Customer shall be responsible for reviewing such occurrences and modifying their backup sets as appropriate.

For confidentiality and security reasons data transmitted cannot be opened or read by any of the MSA Remote Data Protection processes. It therefore remains the Customer responsibility to ensure that data integrity, including virus checking, is maintained.

The Customer shall be responsible for performing all data restore operations.

3.4. Reports

The Customer shall be responsible for reviewing and acting upon the reports provided by the Remote Data Protection service.

The Customer authorized representative shall be responsible for reviewing the detailed logs generated by the Remote Data Protection service.

3.5. Service and Maintenance

The Customer shall accept installation of all product and service releases and engineering changes (hardware, software, or firmware) deemed necessary by MSA to maintain and/or upgrade the Remote Data Protection service.

4. SUPPORT AND ESCALATION PROCEDURE

4.1. Customer Escalation Priorities

The following table defines the escalation priorities to be used by the Customer and MSA in opening calls concerning the Remote Data Protection Service.

<p><u>Priority 3 (Low)</u></p> <p>Classification: General inquiry or problem which has no operational impact on the Customer system.</p> <p>Call Logging: 08:00 to 18:00 hrs weekdays</p> <p>Time to Resolve: 48-72 hours</p>	<p><u>Typical Event:</u></p> <ul style="list-style-type: none"> • Billing or documentation query • Request to move or re-deploy services • General product/functionality inquiry • Report generation issues • General advice and guidance • Product/service enhancements <p>Logged calls shall be serviced on a first-come-first served basis and typically resolved within one day.</p>
<p><u>Priority 2 (Medium)</u></p> <p>Classification: Customer or MSA have identified a possible error or fault with the installed MSA service but which has no critical effect on any other part of the service.</p> <p>Call Logging: 24hr x 7 day x 365 days</p> <p>Time to Resolve: 24-48 hours</p>	<p><u>Typical Event:</u></p> <ul style="list-style-type: none"> • Previously installed and working Remote Data Protection software now not functioning correctly • Problem backing up a single Customer system <p>If logged during business day (08:00 – 18:00 hrs. Monday to Friday) and an immediate resolution is not available the call shall receive attention during the next business day.</p>
<p><u>Priority 1 (High)</u></p> <p>Classification: Customer or MSA have identified a possible error or fault with the installed MSA service which is affecting multiple Customer clients or causing severe impact to system operations.</p> <p>Call Logging: 24hr x 7 day x 365 days</p> <p>Time to Resolve: 0-24 hours</p>	<p><u>Typical Event:</u></p> <ul style="list-style-type: none"> • Escalation of Priority 2 call • MSA remotely monitored fault on leased line • Customer unable to restore data • Customer experiencing MSA related problems backing up from multiple systems <p>Call referred immediately to MSA Project Manager who shall become the primary point of contact and coordinate recovery actions.</p> <p>If problem requires onsite technical support this shall be scheduled with Customer.</p> <p>Every 3-hours MSA management shall review the situation and the MSA Project Manager shall provide a status report to the Customer.</p>

Some calls may require further investigation and even internal escalation by technical specialists. Although MSA intends to resolve an open call in the shortest possible timeframe, this may, in some cases depend on the availability of diagnostic information from Customer. In this case MSA shall monitor events at every stage throughout the diagnostic process and keep Customer informed of progress.

In many cases MSA's operations staff, through their service monitoring systems, shall be aware of problems before they are logged by the Customer. In these cases the operations staff shall call the assigned Customer authorized representative to arrange the necessary remedial action.

Any investigative work carried out by MSA personnel on a fault that is found not to be the responsibility of MSA shall incur charges, with a minimum billable charge of \$250. Should travel and accommodation be involved, this shall also be charged at cost to Customer.

4.2. Disaster Recovery - High Priority

In the event of the Customer invoking a disaster recovery or disaster recovery test, the normal Remote Data Protection Service Level Agreement shall be suspended for the duration of the disaster recovery. During this time the following disaster recovery Service Level Agreement shall be put into effect.

<p><u>Disaster Recovery (High)</u></p> <p>Classification: Customer invokes an onsite disaster recovery.</p> <p>Call Logging: 24hr x 7 day x 365 days</p> <p>Time to Resolve: Problem determination shall start immediately and a recovery plan shall be proposed to Customer depending on the exact nature, location and scale of the problem.</p> <p>Problem resolution activity shall be maintained on a 24-hour basis until the problem is resolved.</p>	<p><u>Typical Event:</u></p> <ul style="list-style-type: none"> • Major data loss • Loss of entire Customer site • Scheduled disaster recovery test <p>Call referred immediately to MSA's Project Manager who shall become the primary point of contact and coordinate the following actions:</p> <ul style="list-style-type: none"> • Notify all relevant members of the MSA management • Review of any previous call history • Interrogation of database and remote diagnostic support systems • Implement repair/replacement/Technical Support Staff procedure • Arrange arrival onsite of MSA Technical Support, if applicable
---	---

	<ul style="list-style-type: none"> • Feedback problem status updates to Customer on a regular basis • Contact Customer to confirm successful resolution <p>If a problem requires an onsite technical visit, this shall be scheduled with the Customer.</p>
--	--

5. PERFORMANCE LEVEL AGREEMENT

MSA acknowledges that the consistent availability and performance of the Remote Data Protection service is essential to ensuring that the Customer's data can be effectively backed up, transferred offsite, and made available for retrieval upon request.

Subject to the product parameters defined in the Remote Data Protection Service Guide and the Customer having fulfilled their obligations under the terms of the SLA, Section 3, the following performance level criteria shall apply:

The service shall be considered to be outside of an acceptable performance level if:

1. MSA goes beyond the time to fix period, i.e. 24-hours, for more than a total of 4-hours (excess outage period) in a calendar month for one or more Priority 1 escalations.

OR

2. If, in the event that the Customer notifies MSA of a site disaster situation requiring the recovery process to be invoked, and MSA cannot restore the Customer's system and data within 24-hours of the call being logged and confirmed, then the Customer shall be credited with an amount equal to one month's current service charge as a credit against the account.