S.M.A.R.T. Managed Services

1. Definitions

The following definitions shall be used for purposes of this Service Level Agreement:

2. Priority Levels

The following table shall be used for classifying issues or requests:

Priority Level	Description
P1	My CRM (Production instance only) is completely down or system-critical functions are inaccessible by users.
P2	My CRM is generally up and functioning, but one or more items are not working as expected.
P3	Non-critical items, configurations, training requests or general questions about the application.

3. Support Levels

MasterSolve shall use commercially reasonable efforts to provide the following support based upon the priority level of the issue or request:

Priority Level	Availability	Initial Response Time	
P1	Telephone/email support	**Maximum SLA:** 2 business hours	**Avg. Response:** 1 business hour
P2	Telephone/email support	**Maximum SLA:** 8 business hours	**Avg. Response:** 4 business hour
P3	Telephone/email support	**Maximum SLA:** 2 business days	**Avg. Response:** 8 business hour

4. Point of Contact

MasterSolve shall designate a point of contact who shall function as the primary contact for technical matters for the Customer Success Team. You may also reach our Customer Success Team directly at support@mastersolve.com.

5. Fees

Support Level	Fees	Payment Term
S.M.A.R.T. Support	Included in Managed Services Subscription Fees	N/A

6. Shared Responsibility

MasterSolve operates on a shared responsibility model with its customers and its cloud-based services providers. Each party — MasterSolve, the customer, and any cloud-based services providers — are accountable for different aspects of security and compliance, and must work together to ensure full coverage.

MasterSolve assumes responsibility for managing physical security and data security on its premises, and on any company-owned networks, computers, or other devices used by its employees. MasterSolve also works closely with its cloud-based services providers to ensure any issues regarding system availability or uptime, or any issues regarding data access or security are escalated to the appropriate support teams on behalf of the customer, so that such issues may be resolved in a timely manner.

The customer assumes responsibility for managing physical security and data security on their premises, and on any company-owned networks, computers, or other devices used by their employees. Customers should carefully consider the services they choose by reviewing their security and compliance policies and by reviewing any applicable laws and regulations pertaining to using such services.

Cloud-based service providers (for example: Salesforce CRM, SugarCRM, Zendesk, etc.) offer their own security policies, which may be published on their websites or may be requested of them directly for review.

Together, this shared responsibility model serves as a framework for physical and data security, where each party has specific responsibilities to help ensure overall coverage.