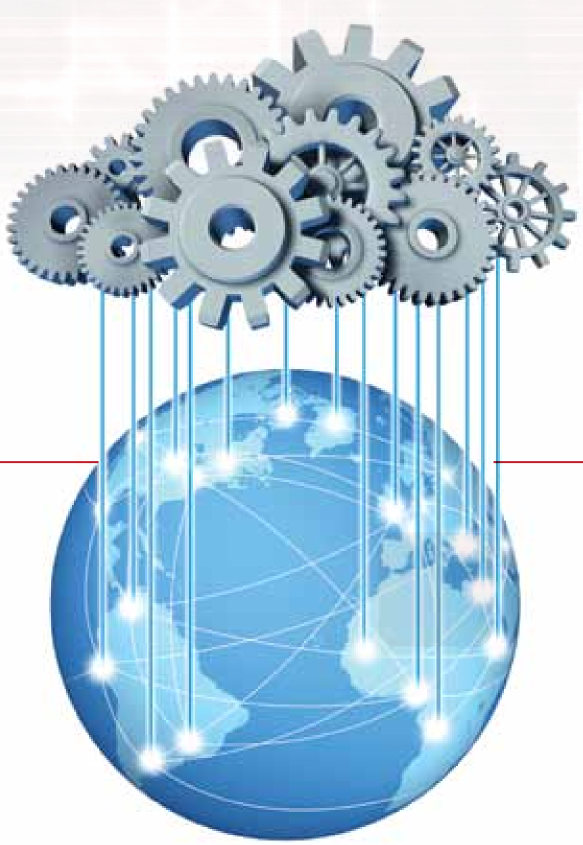
ClaritasCRM™ for Cloud Security



Your Application Security & DATA PRIVACY is our Utmost Priority

We take customer confidentiality seriously. In this datasheet, we like to highlight on how we take various measures to ensure security compliance, and let you have a peace mind knowing that your application and data is in safe hand.

Physical Data Centre

Physical platform is the number one security aspect you need to consider. Claritas™ sit in Microsoft Global Foundation services (GFS) Data Centre which runs in geographically distributed facilities. You should know that you application is sharing hosting spaces and utilities with well-known Microsoft Online Services such as Office365, Hotmail and Windows Live Messenger. Microsoft data Centre are designed to run 24x7 with prevention measures on power redundancy, hardware failure, physical intrusion and network outages. These facilities are managed, monitored and administered by highly qualified operational personnel. Watch the video to learn more about where your application and data is hosted.

Confidentiality

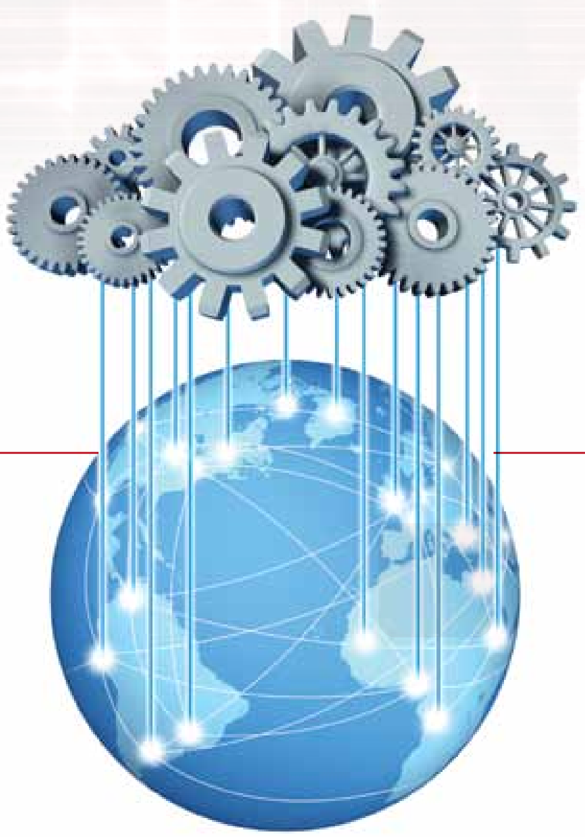
Claritas™ provides confidentiality via SMAPI identity and access management. In short, we ensure that only properly authenticated entities are allowed access to your system. Multi-tenanted data isolation mechanism is also carefully planned and executed for physically and logically segregation of individual customer data. Sensitive data fields such as password and credit card are properly encrypted using MD5 or SHA2, before storing and transmitting across the cloud. Optional SSL or secure HTTP with private key management can be embedded to provide added security features to your application if deemed necessary. Claritas™ framework hypervisor and root OS runs on Windows Azure Fabric Controller which provide network packet filtering that assures spoof traffic or denial-of-service (DOS) attack can be minimized. We allow you to specify fixed IP addresses that is allowed to access to your application, in turns, protecting your application and data being compromised.

This document is for information purpose only. Claritas™ makes no warranties, express, implied, or statutory, as to the information in this document. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced, stored in or transmitted in any form or by any means (electronic, mechanical, photocopying, recording), or for any purpose, without the express written permission of Claritas™.

www.claritascrm.com

Pioneering CRM Innovation

ClaritasCRM™ *for* Cloud Security



Windows Azure

Integrity

Claritas™ sits on top of Microsoft Azure Cloud stack to provide ultimate confidentiality, integrity and availability to your business data. With Microsoft GFS infrastructure, we are ISO 27001 certified and fully committed to Safe Harbor Framework obligations. We enforce customer data segmentation by allowing customer an option to choose a geo-location where their data is stored. We also practices various multitude and strict compliance-enabling features on access control, encryption, availability and privacy – towards our single goal to protect your sensitive information from unauthorized access and changes. While it is the responsibility of customer to ensure business and regulatory compliance, we are committed to help you stay compliance and provide you with the information you need to stay compliance to international and local regulatory standards.

Availability

The main advantages of Claritas™ CRM Cloud Edition are robust availability based on extensive redundancy achieved with virtualization technology. Leveraging on geographically distributed cloud infrastructure, we provides you with a virtual disaster recovery (DR) site with hot-failover capability. Claritas ™ adheres to strict principles of high availability (H/A) through infrastructure redundancy and automatic failover. We automates health monitoring processes to ensure that in the event of any hardware failure, your application instances will be moved to another node to restore the service to full availability. These business continuity and recovery policies are executed transparently so that you do not need to worry or hire dedicated IT specialist to monitor your service status. Even during our regular preventive maintenance, patch or upgrade events are carried with minimal customer interaction.

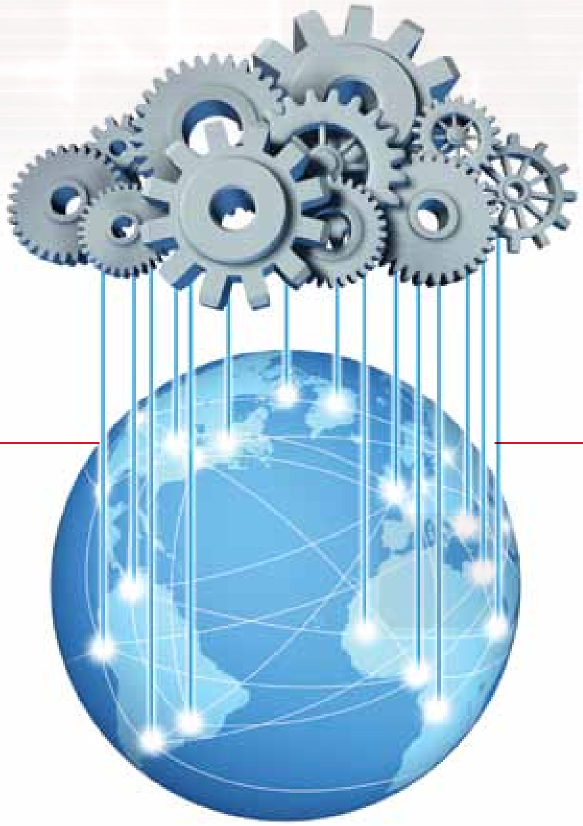
Accountability

We provide transparent accountability to allow you to manage your application exclusively. Claritas™ demonstrates safe operation accountability and traceability to customer data through multiple levels of monitoring, logging and reporting. We aimed to provide true visibility to our customer on data modification or delete, be it intentionally or unintentionally. The Claritas™ audit trail gathers log information of all modules and store in database log.

This document is for information purpose only. Claritas™ makes no warranties, express, implied, or statutory, as to the information in this document. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced, stored in or transmitted in any form or by any means (electronic, mechanical, photocopying, recording), or for any purpose, without the express written permission of Claritas™.

www.claritascrm.com

Pioneering CRM Innovation



ClaritasCRM™ *for* Cloud Security

Data Deletion

We treat data privacy seriously. Your data confidentiality is extended beyond the useful life cycle of your data. When comes to data deletion or migration, Claritas™ complies with proper process on data disposal. Upon termination of your subscription or contract, our support personnel follow rigorous data handling procedures to ensure no copies of your data are kept in primary as well as backup site. Successful execution of delete operation removes all references to the associated data item.

Data Backup and Retention

We provide numerous levels of redundancy to ensure maximum availability to your data. Data is replicated to three separate nodes within the cloud, minimizing the impact of hardware failures. Based on your business needs, system automatically performs periodical data archival and backup to ensure optimal performance of the system. You may also choose to do optional personalized backup where data is periodically extracted from cloud storage to your offsite private storage.

Internal staff

Claritas™ internal staff practices high level of professionalism and integrity when working with customer's application and data. We implement tight access control to sensitive customer data, hence limiting unauthorized access to application, system and network level. Our developer and support follow team follows formal process when they are required to access to confidential customer account or related information, and this is only done with request and acknowledgement from the client. With a combination of multi-tier security access feature, we are able to enhance independent detection of malicious activity that may be a potential threat to your data privacy. Your data security is our utmost priority and you can sit back and realizing your application is thoroughly protected.

This document is for information purpose only. Claritas™ makes no warranties, express, implied, or statutory, as to the information in this document. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced, stored in or transmitted in any form or by any means (electronic, mechanical, photocopying, recording), or for any purpose, without the express written permission of Claritas™.

www.claritascrm.com

Pioneering CRM Innovation