MERIDIAN CLOUD SECURITY STANDARDS

A Complete guide to Meridian Cloud Network and Security

© Copyright 2020 Accruent, LLC

ACCRUENT

TABLE OF CONTENTS

SECTION I: SYSTEM SECURITY 4

SECTION II: AUTHENTICATION 7

SECTION III: PHYSICAL SECURITY 9

SECTION IV: BACKUP & DISASTER RECOVERY 10

SECTION V: INTERNAL POLICIES & PROCEDURES 12

SECTION VI: WEB APPLICATION PROGRAMMING INTERFACE (API) 14

ABOUT ACCRUENT 15

© Copyright 2020 Accruent, LLC

MERIDIAN CLOUD SECURITY

This document offers an overview to the technical infrastructure, features and policies built into Meridian Cloud. It details how security features are implemented within the application and surrounding networks, and functions as a supplemental guide for technical evaluations of the Meridian Cloud infrastructure and software.

© Copyright 2020 Accruent, LLC

SYSTEM SECURITY

System Security encompasses preventive measures that protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction or improper disclosure. Successful network security creates a secure platform (across all physical and software components) for computers, users and programs to perform critical functions within a secure environment. VFA's network security policy encompasses details about overall application architecture, system protocols, encryption, firewalls, antivirus, intrusion and vulnerability management.

This white paper encompasses details about overall application architecture, system protocols, encryption, firewalls, antivirus, intrusion and vulnerability management.

© Copyright 2020 Accruent, LLC

APPLICATION ARCHITECTURE

Platform Design: Meridian Cloud is hosted on the Microsoft Azure platform leveraging best-practice security, scalability and management tools of this platform. Meridian Cloud is built upon multi-tenant SaaS architecture that is designed to segregate and restrict data access for customers based on their business needs.

Software Design - Thin Client: Meridian Cloud is available as a set of light weight web-based applications. The Meridian Cloud requires a modern internet browser on the client side. Because of the architecture, virtually all processing takes place on the server side of the application.

Software Design - Technology: Meridian Cloud utilizes Azure PaaS and SaaS services and the main applications are built upon a combination of C#, AngularJS, ExtJS, HTML5 and JavaScript.

Minimum Bandwidth (Cloud-Hosted): See System Requirements Document.

Required Browser Add-Ins: An optional client component can be used to streamline the data communication to the user's PC and optimize the user experience with other applications installed on the user's PC. This optional add-on can be downloaded from the Meridian Cloud homepage.

Software Configuration: Meridian Cloud is designed around feature-rich industry best practices related to engineering document management where features can be enabled and disabled based on organization needs and configuration options are available for those elements that are unique to an organization.

Email Notifications: Meridian Cloud utilizes a SendGrid email system for workflow and system notifications.

Data Architecture and Logic: Data architecture is contained within Microsoft Azure and uses a combination of databases, such as SQL Azure, for structured data and blob, and table storage or unstructured data.

External cloud services are used elements like searching indexing (Elastic Cloud) and Viewing (Autodesk Forge).

© Copyright 2020 Accruent, LLC

PROTOCOLS

Transmission Control Protocol / Internet Protocol (TCP/IP): The Meridian Cloud application is web-based, so it requires active internet or intranet sessions (HTTPS) over TCP/IP and IPv4 or IPv6.

ENCRYPTION

Data in Transit: Data sent is always encrypted, and the application runs on HTTPS.

- Encryption Level: Data is encrypted upon application login utilizing Transport Layer Security (TLS) 1.2. Secure.
- Data at Rest: By default, database information is stored on our secure Azure servers and is encrypted at rest. Unstructured data is stored using Azure blob storage and is also encrypted at rest.

FIREWALLS

Ports: The port and protocol requirements needed to enable the application to operate on the Client and the Server sides HTTPS (Port 443), HTTP (Port 80) is only used for forwarding to Port 443. FTPS ports are used for large data migrations and can be enabled upon request for a single customer.

All calls from on-premises systems to the Meridian Cloud are outbound calls. Meridian Cloud does not make any calls to on-premises installation and it doesn't have any knowledge regarding its location.

ANTIVIRUS

All Meridian Cloud servers are equipped with an antivirus software which is part of the application monitoring.

Penetration Testing: External penetration testing is conducted on a yearly basis. Internal security testing happens on a continuous basis.

Vulnerability Management: During penetration testing, network layer vulnerability scans are also performed to identify weaknesses within the application as well as the infrastructure and the OS layers.

Vulnerability Classification: Security issues are classified into low, medium and high priority incidents in alignment with production team and organizational leaders.

© Copyright 2020 Accruent, LLC

AUTHENTICATION

Authentication is one of the most basic and top-layer security requirements, as it establishes the identity and credentials of the user accessing the system. Access to the Meridian Cloud requires authentication via one of the supported methods, including SAML based Federation, Social Login or OpenID Connect. Tenant administrators can configure as many identity providers as needed to support their business use cases.

Meridian Cloud utilizes new-user approvals, account management, session timeouts, and more to manage overall authentication and controls.

© Copyright 2020 Accruent, LLC

GENERAL

Authentication Type: Meridian Cloud supports a variety of authentication providers including Google, Microsoft and Office 365/ Azure authentication. Oauth2 compatible authentication can be configured to allow single sign-on (SSO) and MFA scenarios, if required. Meridian Cloud does not store any login user names and passwords as the Identity Providers solely handles this.

USER & PASSWORD MANAGEMENT

User Account Controls: User accounts and groups are maintained by the customer and its tenant administrators. Meridian Cloud allows users that no longer require access to the tenancy to be disabled.

User Invites: Tenant administrators can invite new users from within the system and specify their default access level. Invited users will receive an email that is valid for 30 days to accept the invite. Users that accept the invite can log in using any of the configured authentication providers. Invites sent out to users can be retracted if user had not accepted it yet.

Access Groups and User Right Control: Roles provide a dynamic grouping function of permissions associated with data manipulation or specific application level functions.

Meridian Cloud has a fixed set of roles per data type that can be used for role assignments. Role assignments can involve groups or users and can be made against single projects with defaults per project type. For as-built data, assignments can be made globally, regionally or on-plant level.

All functions of the Meridian Cloud application are controlled by means of the role assignments, therefore users who do not have the appropriate permissions, will not be aware of the existence of certain features, since the tabs, icons or buttons will not be present in their view of the application.

Access Group Basics: Access Groups control the different actions that can be taken by users within the application. This includes the right to view, edit, approve and create any object or module within Meridian Cloud. Up to a 1000 Access groups can be created.

Customers are responsible for the data, content and information it stores on Accruent systems.

© Copyright 2020 Accruent, LLC

PHYSICAL SECURITY

The Meridian Cloud production servers are hosted in Microsoft Azure data centers with the state-of-the-art hosting facilities, including round-the-clock on-site technical staff actively managing, maintaining, and supporting the network, the services it provides and the customers it connects.

PHYSICAL CONTROL METHODS

Colocation Environment: All Meridian Cloud production environment information is held within a colocation environment that is fully SSAE 16 SOC 1 and SOC 2 Certified. Reports can be downloaded from the Microsoft website. https://www.microsoft.com/en-us/trustcenter/Compliance/soc

Authorized Personnel Controls: Accruent does not have any physical access to the product.

MULTI-TENANT DESIGN (CLOUD ONLY)

Multi-Tenant vs. Single Tenant Design: Meridian Cloud utilizes a combination of single-tenant and multi-tenant services where customers hosted on the cloud environment share storage and compute resources.

Microservices Architecture: The Meridian Cloud environment is designed to conform with best practices of microservices architecture. This enables the development team to continuously deliver and deploy large and complex application. Employing microservices architecture improves maintainability, testability and deploy-ability. It also eliminates long-term commitment to a technology stack and enables the development teams to innovate and improve services independently.

Virtualization: Our platform is built on a combination of virtualized machines on Microsoft Azure and uses a series of Azure PaaS and IaaS services.

Data Isolation: Although it is a multi-tenant application, our cloud environment provides data separation by connecting all customer data to a unique tenancy ID, ensuring that all tenant information is separated.

Data Geographical Storage Location: The Azure datacenter region used to host a tenancy is selected on account activation. All customer data stays within the selected region and is not transferred to other data centers outside of the region.

Old Data Disposal and Old Customers: If a client ceases utilization, Accruent reserves the right to remove all data after 35 days.

© Copyright 2020 Accruent, LLC

BACKUP & DISASTER RECOVERY

In the very unlikely event of a data center or individual equipment failure, Meridian Cloud has failover procedures in place to alert customers, reduce downtime, speed recovery and backup data.

© Copyright 2020 Accruent, LLC

DISASTER RECOVERY (DR)

Recovery Point Objective (RPO): Our RPO is 24 hours.

Recovery Time Objective: (RTO): RTO is up to five (5) days in the event of a major catastrophe.

Uptime: Accruent warrants a minimum availability of 98.5% or better per calendar month, except the planned 'downtime' for system maintenance. See the SLA for scheduled downtime windows.

Security Incident Response Plan: There are documented procedures in place for responding to an information security incident.

In the event of an incident, a formal reporting procedure exists detailing whom to contact and through what channels (including authorities if necessary). Post-incident, a root cause analysis of the incident is reported that will include the cause of incident, the immediate resolution and steps that will be taken to prevent similar incidents in the future.

More Info: For more information, please see our formal disaster recovery policy document, which is reviewed on a yearly basis

DATA BACKUPS

Daily backups: All customer data is backed up on a daily basis and stored in a separate Geo-Redundant Storage account.

Backup Frequency: Backups are performed daily between the hours of 2:00-5:30 a.m. CET.

Backup Access: Only authorized Accruent personnel have access to the database backups.

Backup retention: The backup retention time is 14 days.

Application logs retention: The customer specific application logs are removed when tenancy is deleted. Logs backup retention time is 35 days.

System logs retention: The system logs are retained for 360 days.

© Copyright 2020 Accruent, LLC

INTERNAL POLICIES & PROCEDURES

Accruent's commitment to security and compliance is evident in the company's system-wide processes, professional development and training, and overall customer service and satisfaction. Meridian Cloud's security and access control policies reflect the Accruent's ongoing prioritization of product, infrastructure and network regulation.

SECURITY POLICIES

Cloud Infrastructure Updating Policy: Normal priority patches are deployed monthly. Emergency patches will be expedited.

Change Management: All production changes and patches are registered and documented.

Customer Notification: Accruent notifies tenants when material changes are made to information security and/or privacy policies.

Third Party Compliance: All third parties, undergo their own independent testing and adherence to SSAE 16 SOC 1 and SOC 2 compliance, as well as HIPPA and several other compliance measures. Additional information is available upon request, and individual reports are available upon the signage of an NDA.

© Copyright 2020 Accruent, LLC

ACCESS CONTROL POLICY

Internal Management VPN: Our cloud environment is managed remotely through a secure VPN. All authorized personnel receive their personal VPN access certificate which can and will be revoked when access is not needed anymore. Monthly access reviews are performed, as well as reviews upon hiring and termination of Meridian Cloud employees. Reviews of production access privileges are performed periodically by Accruent. All secrets are safely stored on a dedicated secrets management system which controls access to admin credentials and passwords.

All access permissions (internal network and Azure) are integrated with our Active Directory domain. Domain policy enforces a mandatory password change every 90 days. If passwords are not changed, access is revoked.

Accruent's password policy specifies that at least ten (10) characters with three (3) complexity clauses are used for all production service accounts.

Remote Devices: We have specific standards for general teleworking devices that connect via a web application. Only approved devices have remote access to the production environment.

© Copyright 2020 Accruent, LLC

WEB APPLICATION PROGRAMMING INTERFACE (API)

The Meridian Cloud Web API is an interface that can be used for three primary functions: GET, POST and PUT. The GET method retrieves information and is used to retrieve specified results. The POST method creates NEW records through the API and inserts them into the database. The PUT method updates/replaces data on EXISTING records.

The API can be used for simple tasks link retrieving and updating document and asset information.

Special Analytics databases connections are available for data analytics using tools like PowerBI. The databases can be setup on a sub-set of a copy of the actual system data.

All API calls are authenticated and audited. API access license is required to utilize the Meridian Cloud API.

© Copyright 2020 Accruent, LLC

ABOUT ACCRUENT

Founded in 1995, Accruent is headquartered in Austin, Texas, and serves a wide range of industries in 150+ countries around the world. Accruent is the largest company focused on optimizing every aspect of planning and managing your physical resources. Accruent's product portfolio is designed for the complex needs of specific industries, including: corporate real estate, healthcare, higher education, public sector, retail, telecom, and utilities.

DISCLAIMER

Accruent reserves the right to revise this publication from time to time and to make changes in the content hereof without obligation to notify any person of such revisions or changes.

CONTACT FOR A DEMO

Accruent, LLC
sales@accruent.com | www.accruent.com | 512-861-0726

© Copyright 2020 Accruent, LLC