Information Security & Governance Declarations

Last Update: 03/15/22

Table of Contents

GOVERNANCE

Q: Describe your organization's information security program, including the supporting governance policies, standard operating procedures, and roadmap for strategic initiatives and future investments.

A: Our information security protocol relies on standardized training procedures, limiting employee access to Client information based on their job responsibility and scope of training, and regular training.

Meridia's development team and project managers are the only groups that, depending on the contracted responsibilities, may have access to the Client information, or data.

Typically, Client chooses their CloudVOTE usernames and passwords. Only the usernames are visible and available to assigned Meridia staff, who are restricted to only be able to reset the Client's password, but are never able to obtain it.

Q: Describe your organization's internal audit, risk management, or compliance department responsibilities for conducting periodic audits of the design and effectiveness of internal controls, including frequency of audits and remediation activities.

A: Meridia manages and mitigates risk in context of the CloudVOTE solution by ensuring that the policies and procedures set by Microsoft Azure's hosting platform are not compromised on company level.

Employee training, development quality assurance and security protocols are the main tools in maintaining minimal risk levels.

Periodic audits (quarterly and annual) ensure proactive approach to discovery of any security issues. We prioritize and immediately review incident logs and system reports to ensure the level of compliance and response contracted for the CloudVOTE system.

Q: Describe any pre-employment screening that your organization perform on workers (employees and contractors), such as: background checks, reference screenings, education verification, and drug testing.

A: Meridia performs reference screening on all third-party (outsourced) resources. We do background checks, personal and professional reference review for all in-house resources.

All in-house resource screening is performed by HRM Consulting Ltd., Buffalo Grove, IL

Q: Describe the security awareness training your organization provides to workers (employees and contractors), such as: Phishing, Spam, Virus/Malware, Social Engineering, AML, Acceptable Use, etc.

A: Information security training covers phishing/spam, virus/malware, privacy and acceptable use programs.

Initial training is supplemented by ongoing updates on current threats and vulnerabilities, as well as periodic re-training for all employees.

Q: Describe your organization's record information management (RIM) process and how Client data is managed throughout the relationship and how it is returned and/or purged from internal systems at the end of the contract.

A: Records are stored in a cloud-based service (Citrix ShareFile) with access restricted to assigned project managers and development team.

Records containing Client's personal, or sensitive information are returned, and local copies destroyed within five (5) business days of written termination of the contract.

INFORMATION ASSET MANAGEMENT

Q: Describe the hosting model used to deploy your organization's product or service (e.g. Private/Public/Hybrid Cloud, On-Premise, etc.).

A: Meridia deploys and hosts the CloudVOTE content management and audience response system on Microsoft Azure.

Client has two hosting options:

1) Shared/Multi-Tenant Hosting (default)

2) Dedicated/Single-Tenant Hosting (available upon request, at additional cost)

Q: Describe your organization's commitment to data privacy including internal policies and procedures related to protecting personally identifiable information (PII) and Personal Health Information (PHI) that is provided to you by Clients.

A: Client's CloudVOTE instances meet most information security compliance requirements. Read more at https://www.cloudvote.com/security.

CloudVOTE does not explicitly store any PII or PHI. On a case-by-case basis, based on specific agreements between a Client and Meridia Interactive Solutions, certain, limited PII can be stored in CloudVOTE for syncing (matching) the polling session information with Client's external LMS.

Q: Can Clients define the legal jurisdictions where their data can be transmitted, processed, and stored?

A: Client's CloudVOTE deployment defaults to MS Azure US-East or US-West regional centers with automatic redundancy backups elsewhere in the US.

Per Client's direction and contract, their CloudVOTE instance can be hosted in any of the current MS Azure regional centers.

Q: Describe your organization's data classification schema (e.g. public, confidential, proprietary, etc.) and the level of data protection applied for each designated class.

A: - Public. general company information, publicly available on the website

- Limited protection. Generally accessible by website visitors, customers, and employees

- Confidential/Proprietary. Meridia R&D data, accounting & contractual information

- Restricted access. Employees have access to a limited number of designated documents and/or groups of documents depending on their assignment to an individual Client/Project.

- Owners and management has secure access to all documents and projects across all departments.

Q: Explain how your organization's product or service is architected to segregate customer data to ensure integrity and confidentiality.

A: Client's information is segregated and protected in CloudVOTE's default (Multi-Tenant) environment by separation of databases and individual logins.

Client can opt-in (at additional cost) to deploy CloudVOTE to a Single-Tenant environment, dedicated exclusively to their instance.

Q: Describe your organization's encryption key management process and procedures (e.g. PKI, certificate authority, key distribution, and rotation).

A: Software encryption keys are only distributed and included in the application development by and for dedicated personnel.

Encryption keys for the public website are not available to any employee and are not stored on the corporate network, or in file storage.

All Client information, private, confidential or security-related data is stored and encrypted in Citrix ShareFile.

Q: Describe how your organization uses encryption to protect confidential data while it is in transit, stored, or archived (for example in a backup system).

A: Client's data is protected by Citrix ShareFile's integrated encryption methods. Meridia does not store any Client information, private, confidential or security-related data locally or outside of Citrix ShareFile system.

Q: Describe your organization's Data Loss Prevention (DLP) strategy and the control measures implemented to actively prevent unwanted egress flow of Client data.

A: CloudVOTE is not hosted on-premise. Backup & Resiliency Standard Response documentation can be found at www.cloudvote.com/security

Q: Describe your organization's hardware and software inventory processes, procedures and tools and how they ensure that newly introduced hardware and software are accurately reflected.

A: CloudVOTE is not hosted on-premise. Physical and Information Security Standard Response documentation can be found at www.cloudvote.com/security

Q: Describe the processes in place to detect rogue devices and software when they are introduced in the environment.

A: CloudVOTE is not hosted on-premise. Physical and Information Security Standard Response documentation can be found at www.cloudvote.com/security

Q: Do you scan attachments in emails before they are placed in the user's inbox? If so, please describe how you scan and block all e-mail attachments entering the organization's e-mail gateway if they contain malicious code or file types that are unnecessary for the organization's business. Is this scanning done before the e-mail is placed in the user's inbox? Does this include e-mail content filtering and web content filtering?

A: Meridia uses Standard Security & Protection measures and protocols in Office365. More information is available at: https://products.office.com/en-us/business/office-365-trust-center-security

ACCESS CONTROL

Q: Describe your organization's access provisioning process for new hires and transferring workers (employees and contractors), including how this is formally authorized and commensurate with their job responsibilities.

A: Meridia assigns user access based on contractual requirements, regardless of the employee being a new hire, or an existing staff.

All CloudVOTE-related security concerns are addressed in Physical and Information Security Standard Response documentation at www.cloudvote.com/security

Each employee is given a domain username and password, which allows access to corporate data associated with their role & responsibilities.

If an employee is assigned to a specific Client/Project, they gain access to secure Citrix ShareFile location pertaining to the assignment.

Transferred and terminated employees lose access to their email, domain and all data immediately.

Access privileges are taken over by the immediate supervisor, on an as-needed basis until a replacement staff is identified and trained.

Q: Describe your organization's access removal processes for terminated and transferred workers (employees and contractors), including how this is formally tracked and associated information assets are returned.

A: Transferred and terminated internal (corporate) Meridia staff immediately loses access to all internal and external resources, including, but not limited to email, Citrix ShareFile, and domain resources.

All CloudVOTE-related security concerns are addressed in Physical and Information Security Standard Response documentation at www.cloudvote.com/security.

Q: Describe your organization's process for managing inactive user accounts for both end users and administrators.

A: Meridia holds internal (corporate) inactive accounts for thirty (30) days and removes them after sixty (60) days.

All CloudVOTE-related security concerns are addressed in Physical and Information Security Standard Response documentation at www.cloudvote.com/security.

Q: Describe your organization's process for performing periodic account reviews, including frequency, responsibilities, and remediation action taken for inappropriate access identified.

A: Meridia performs quarterly and annual account access review, as well as immediate review of any unauthorized access based on automated security reports and logs.

CloudVOTE account security concerns are addressed in Physical and Information Security Standard Response documentation at www.cloudvote.com/security.

Q: Describe how your organization restricts remote access to the company's network, including administrator access, direct database access, backdoors, APIs, or other methods that would allow non-standard access to Client-related data.

A: Meridia ensures restricted access to company's premises, servers and network equipment, as well as strong password rules for workstation, Wi-Fi and network access.

CloudVOTE Microsoft Azure deployment security concerns are governed by Physical and Information Security Standard Response documentation at www.cloudvote.com/security.

Q: Describe what capabilities your solution or service has for access federation, multi-factor authentication (MFA), and IP restrictions?

A: Multi-Factor Authentication and IP access restrictions are available to all CloudVOTE tenants in both Single-Tenant and Multi-Tenant environment.

Q: Describe your organization's minimum password requirements in terms of character length, complexity, history, rotation period, lockout, timeout settings, and how they are stored.

A: Meridia can provide access restrictions based on soft-configured number of attempts and retry timeout.

Meridia uses Microsoft Entity Framework Core. The framework provides settings to set password length, expiry etc. restrictions.

CloudVOTE Microsoft Azure deployment security concerns are governed by Physical and Information Security Standard Response documentation at www.cloudvote.com/security.

Q: Describe how your organization manages administrator-like accounts access, including the account checkout process, auditing, and how any shared account credentials are stored.

A: CloudVOTE deployment uses Client-configured "Master" account for administrative access to all "Child" accounts configured for the Client's instance.

Audit logs can be sent to the Client directly, monitoring access and any potential security breaches.

Q: Describe whether user or system accounts are shared amongst workers (employees or contractors) and the controls that are in place to prevent misuse.

A: No. Meridia prohibits shared/system accounts on the internal (corporate) level.

CloudVOTE Microsoft Azure deployment security concerns are governed by Physical and Information Security Standard Response documentation at www.cloudvote.com/security.

Q: Describe the number of users and groups within your organization that will have access to in-scope systems that will process and store Client data.

A: Meridia expects five (5) users to have some level of access to Client's data stored off premises, inside Client's CloudVOTE instance.

Three (3) of those users will have permanent access (individually separated from one another)

Two (2) users will be temporary and their access will be removed upon completion of the development phase of the project.

REGULATORY COMPLIANCE & CERTIFICATIONS

Q: Describe any government regulation or industry standards that your systems or service complies with (e.g. PCI, ISO, SSAE-16, SOC2, etc.), along with related certifications. Please provide copies of the latest reports and/or certifications.

A: CloudVOTE Microsoft Azure compliance and certification can be found via Physical and Information Security Standard Response documentation at www.cloudvote.com/security.

Q: Describe the type of audits your organization allows Clients to perform.

A: N/A

CloudVOTE Microsoft Azure deployment audit restrictions are governed by Physical and Information Security Standard Response documentation at www.cloudvote.com/security.

INCIDENT RESPONSE

Q: Describe your organization's incident and problem management strategy, including communication and escalation procedures followed by the Security Operations Center (SOC) or Computer Security Incident Response Team (CSIRT).

A: CloudVOTE Disaster Recovery Standard Response can be found at www.cloudvote.com/security.

Q: Describe how your organization tracks information security events to ensure they are reviewed, prioritized, assigned, and remediated in a timely manner.

A: CloudVOTE Disaster Recovery Standard Response can be found at www.cloudvote.com/security.

Q: Describe when your organization will notify Clients of a security breach which may have resulted in the loss of Client data or the compromise of in-scope systems.

A: CloudVOTE Disaster Recovery Standard Response can be found at www.cloudvote.com/security.

Q: Describe your organization's ability to produce electronic forensic investigative information that is authentic and unaltered.

A: CloudVOTE Disaster Recovery Standard Response can be found at www.cloudvote.com/security.

Q: Describe how your organization will assist with any e-discovery, legal hold, and forensic investigation requests.

A: CloudVOTE Disaster Recovery Standard Response can be found at www.cloudvote.com/security.

NETWORK SECURITY

Q: Describe the controls your organization has implemented to secure data communications (e.g. email, data transfers, etc.) to prevent unauthorized access.

A: CloudVOTE Microsoft Azure deployment secure data communication rules are governed by Physical and Information Security Standard Response found at www.cloudvote.com/security.

Q: Describe how your organization's network architecture and segmentation have been configured to support information security best practices.

A: CloudVOTE Microsoft Azure deployment network architecture rules are governed by Physical and Information Security Standard Response found at www.cloudvote.com/security.

Q: Describe your organization's use of Firewalls, including Web Application Firewalls (WAFs) and how they have been set up to prevent unwanted access to in-scope system and Client data by both internal and external connections.

A: CloudVOTE Microsoft Azure deployment use of firewalls is governed by Physical and Information Security Standard Response found at www.cloudvote.com/security.

Q: Describe how your organization uses Intrusion Prevention Systems (IPS) and/or Intrusion Detection Systems (IDS), including how they have been configured to drop suspicious or unwanted network packets, and to alert on unauthorized ports, protocols and services.

A: CloudVOTE Microsoft Azure deployment IPS and IDS rules are governed by Physical and Information Security Standard Response found at www.cloudvote.com/security.

Q: Describe your organization's approach to performing penetration testing, including the scope, frequency, who it is conducted by, and how risks are addressed.

A: CloudVOTE Microsoft Azure deployment penetration testing is governed by Physical and Information Security Standard Response found at www.cloudvote.com/security.

Q: Does all your wireless traffic use Advanced Encryption Standard (AES) encryption with at least Wi-Fi Protected Access 2 (WPA2) protection? If not, please explain.

A: Yes, as it relates to internal, corporate infrastructure.

CloudVOTE Microsoft Azure deployment communications encryption standards are governed by Physical and Information Security Standard Response found at www.cloudvote.com/security.

Q: Are Bluetooth and wireless peer-to-peer services disabled?

A: Yes, as it relates to internal, corporate infrastructure.

CloudVOTE Microsoft Azure deployment use of Bluetooth and peer-to-peer devices is governed by Physical and Information Security Standard Response found at www.cloudvote.com/security.

Q: Are BYOD and untrusted devices placed in an isolated wireless network (internet access for BYOD via own VLAN)?

A: Yes, as it relates to internal, corporate infrastructure.

CloudVOTE Microsoft Azure deployment use of BYOD and untrusted devices is governed by Physical and Information Security Standard Response found at www.cloudvote.com/security.

INFRASTRUCTURE SECURITY

Q: Describe your organization's process for hardening infrastructure (e.g. servers, databases, and network components), prior to deployment that will support the management of Client data.

A: CloudVOTE Microsoft Azure deployment infrastructure hardening rules are governed by Physical and Information Security Standard Response found at www.cloudvote.com/security.

Q: Describe how your organization performs vulnerability scanning of its infrastructure (e.g. servers, virtual machines, etc.), including: the scanning tools used and the frequency of scans.

A: CloudVOTE Microsoft Azure deployment vulnerability scanning rules are governed by Physical and Information Security Standard Response found at www.cloudvote.com/security.

Q: Describe how your organization tracks, prioritizes, implements action plans, and remediates vulnerabilities identified.

A: CloudVOTE Microsoft Azure deployment action plans are governed by Physical and Information Security Standard Response found at www.cloudvote.com/security.

Additionally, as part of the contractual process, Meridia and the Client agree on a specific set of escalation rules and chain of contacts that support the Client's mission objective.

Q: Describe your organization's process to monitor and apply software patches for operating system, middleware, database and application layers to keep them current and on supported versions. Who is responsible to apply patches?

A: CloudVOTE Microsoft Azure deployment software patch monitoring and application is governed by Physical and Information Security Standard Response found at www.cloudvote.com/security.

Additionally, as part of the contractual process, Meridia and the Client agree on specific rules and limitations of the patching process as it relates to severity levels and escalation rules.

Q: Describe your organization's strategy for managing virus and malware threats at each infrastructure endpoint (e.g. servers, laptops, mobile devices, etc.).

A: CloudVOTE Microsoft Azure deployment virus and malware management is governed by Physical and Information Security Standard Response found at www.cloudvote.com/security.

Q: Describe how your organization's policy or program to manage removable media and mobile devices (laptops, phones, CDs, external hard drives, USB drives, etc.).

A: CloudVOTE Microsoft Azure deployment removable media and mobile device management is governed by Physical and Information Security Standard Response found at www.cloudvote.com/security.

Q: Describe how your organization manages hardware life-cycling practices, including IT asset disposition at end of life.

A: CloudVOTE Microsoft Azure deployment hardware life-cycle practices are governed by Physical and Information Security Standard Response found at www.cloudvote.com/security.

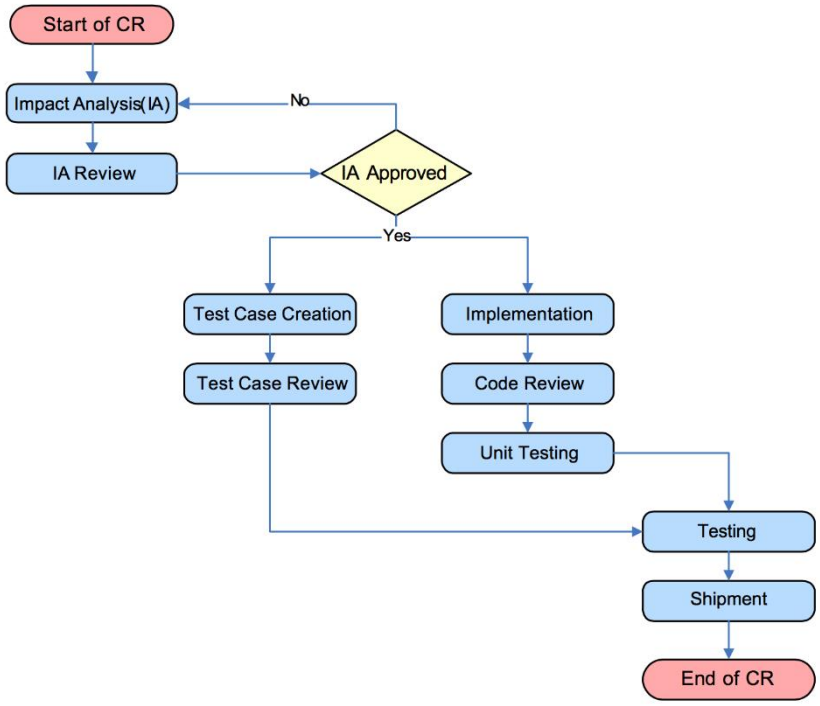
Q: Describe the processes for maintaining the integrity of secure configurations for hardware and software and how you go about proactively detecting and addressing configuration drift.

A: CloudVOTE Microsoft Azure deployment secure configurations and configuration drifts are governed by Physical and Information Security Standard Response found at www.cloudvote.com/security.

CHANGE MANAGEMENT

Q: Describe your organization's change management process for in-scope systems, including how changes are tracked, reviewed, tested, approved and migrated to production.

A: As part of the contractual process, Meridia and Client agree on a set number of revisions included in the initial system deployment.



Change Order form is completed by the Client in case a new requirement, feature improvement or bug fix is needed.

Meridia uses JIRA for change-tracking purposes.

We have specialized teams that excel in implementing change request on systems that are already in production. We work in accordance with the Service Level Agreements signed with the Client against problems of different severity levels. Meridia has implemented the process of Impact Analysis and Root Cause Analysis for problem identification and resolutions. We can maintain different versions of the systems using elaborate SCM processes and tools. We ensure that baselines for different changes are properly identified and changes to code are properly monitored and controlled. Following is the basic flow of a change request:

Q: Describe how your organization uses separate environments (production vs. non-production) in the change management process.

A: Meridia develops all software in a separate, Single-Tenant MS Azure environment, independent of any other Client's instances.

All changes are deployed to this "Staging" environment first for QA testing and any applicable code revisions.

Client may obtain temporary access to the system on an as-needed basis to perform release acceptance testing.

Once release is accepted, the primary (production) environment is updated per contractually agreed-upon schedule and notification rules.

SOFTWARE DEVELOPMENT

Q: Describe the software development process followed by your organization's development staff, including the development methodology used (e.g. RAD, Waterfall, Agile, etc.), and how it incorporates secure software development practices.

A: Meridia uses JIRA and BitBucket secure, hosted development tools to create, manage and release software. Meridia develops using Agile methodology, which ensures quick and responsive approach to all Client's needs.

Meridia maintains different environments and code commit/approval process. Meridia has a development, staging, and production environment. And for data separation, some Clients have their own separate environment as well. Code is fully tested through a strict change management procedure. QA is involved at each level and shipment assurance is done when a new feature is moved from one environment to the other by QA or application specialists.

Q: Describe your organization's policy and practices regarding use of a Client's production data in non-production environments, such as your employee desktop systems or systems used for development, testing, or QA.

A: Meridia never uses, stores, or otherwise manipulates Client's production data in a non-production environment.

During a release testing period, non-production environment will be used to create, store and manage "test" data, which is temporary in nature and will not be retained past the duration of the test.

Q: Describe how your organization performs code scanning (e.g. peer reviews, dynamic, static scanning, etc.) including the technology tools used and how identified security flaws or defects are remediated.

A: Meridia performs code scanning in three stages: 1) developer runs a smoke test in a single test environment 2) QA runs compatibility test on all supported environments 3) project manager runs functionality tests against all recorded issues/sprints.

Defects are reported to the development team directly in JIRA and immediately prioritized and resolved according to agreed-upon schedule.

Q: Describe how your organization's software developers are adequately trained in secure software development practices (e.g. input validation, OWASP, etc.).

A: Meridia employs software development professionals with CMMI Level 2, ISO 9000:2001, and HIMSS Healthcare Security certification. Moreover, we require ongoing technology and compliance training from all resources dedicated to a specific Client's project that requires it.

LOGGING & MONITORING

Q: Describe the type of system events that audit logs are configured to capture for monitoring and alerting (e.g. login attempts, administrator changes, etc.).

A: CloudVOTE Microsoft Azure deployment offers a variety of logging capabilities, including, but not limited to:

- Control/management logs - give visibility into the Azure Resource Manager CREATE, UPDATE, and DELETE operations. Azure Activity Logs is an example of this type of log.

- Data plane logs - give visibility into the events raised as part of the usage of an Azure resource. Examples of this type of log are the Windows event System, Security, and Application logs in a virtual machine and the Diagnostics Logs configured through Azure Monitor.

- Processed events - give information about analyzed events/alerts that have been processed on your behalf. Examples of this type are Azure Security Center Alerts where Azure Security Center has processed and analyzed your subscription and provides concise security alerts.

All CloudVOTE Microsoft Azure deployment logging is governed by CloudVOTE Physical and Information Security Standard Response documentation located at www.cloudvote.com/security.

Q: Describe how your organization ensures important audit logs (e.g. application, database and operating system) are tamper resistant and identify the duration they are retained or archived.

A: All CloudVOTE Microsoft Azure deployment logging is governed by CloudVOTE Physical and Information Security Standard Response documentation located at www.cloudvote.com/security.

Q: Describe how your organization performs log collection/aggregation for review and alerting purposes, including the technologies used (e.g. Splunk, LogRhythm, ArcSight, etc.) and integration with CSIRT or SOC teams.

A: All CloudVOTE Microsoft Azure deployment logging is governed by CloudVOTE Physical and Information Security Standard Response documentation located at www.cloudvote.com/security.

PHYSICAL & ENVIRONMENTAL

Q: Identify the physical locations (e.g. operations facilities, SOC, data centers, etc.), including any third-party locations where in-scope systems and Client data will reside.

A: No on-site CloudVOTE deployment exists.

All CloudVOTE instances are hosted in Microsoft Azure regional centers (and their backups).

Q: Describe your organization's process to administer and manage visitor access to corporate facilities, including identification verification, sign-in/out, escorting, and access log reviews.

A: All CloudVOTE Microsoft Azure deployment physical security rules are governed by CloudVOTE Physical and Information Security Standard Response documentation located at www.cloudvote.com/security.

Q: Describe the preventative and detective physical security control mechanisms (e.g. CCTV, mantraps, guards, locked doors, etc.) your organization has implemented to protect facilities that store and process Client data.

A: All CloudVOTE Microsoft Azure deployment physical security rules are governed by CloudVOTE Physical and Information Security Standard Response documentation located at www.cloudvote.com/security.

Q: Describe the environmental controls (e.g. fire suppression, HVAC, UPS, generators, raised floors, etc.) your organization has implemented to ensure availability of systems that host Client data.

A: All CloudVOTE Microsoft Azure deployment physical security rules are governed by CloudVOTE Physical and Information Security Standard Response documentation located at www.cloudvote.com/security.

RESILIENCY

Q: Describe your organization's data backup strategy including how you monitor backup jobs or real-time data transfers to verify the ability to restore.

A: All CloudVOTE Microsoft Azure deployment backup and resiliency rules are governed by CloudVOTE Resiliency & Backup Standard Response documentation located at www.cloudvote.com/security.

Q: Describe your organization's Service Level Agreement (SLA) provided to Clients for your product or service offering to ensure availability.

A: See attached "Required Service Levels and Service Level Credits - Sample".

Q: Describe your organization's Business Continuity and Disaster Recovery (BCP/DR) strategies for your IT systems, including the frequency of plan tests and policy updates.

A: All CloudVOTE Microsoft Azure deployment backup and resiliency rules are governed by CloudVOTE Resiliency & Backup Standard Response documentation located at www.cloudvote.com/security.

Q: Describe your organization's use of Business Impact Analysis (BIA), specifically the recovery time (RTO) and recovery point objectives (RPO) specific to IT systems supporting Client data.

A: All CloudVOTE Microsoft Azure deployment backup and resiliency rules are governed by CloudVOTE Resiliency & Backup Standard Response documentation located at www.cloudvote.com/security.

Q: Describe the process of backing up systems and data, addressing these specific questions:

How are the systems backed up?

How often are the systems backed up?

Are there offline backups available?

How do you test the integrity of your offline backups and how often?

What is the process you follow when backups fail?

A: All CloudVOTE Microsoft Azure deployment backup and resiliency rules are governed by CloudVOTE Resiliency & Backup Standard Response documentation located at www.cloudvote.com/security.

CLOUD COMPUTING

Q: Describe your capabilities to retain, restore, return, purge and destroy customer data.

A: Client using CloudVOTE can manage data (including archival, restoration and deletion) on their own without Meridia's input or control.

Meridia can guarantee timely data purge/destruction if requested by the Client.

Q: As a consumer of your cloud solution can Client opt in or out of service pack upgrades? Are some upgrades mandatory and others optional?

A: Yes, partially.

Meridia has no control over Microsoft Azure emergency/critical/urgent infrastructure maintenance, thus cannot guarantee certain service packs and patches will not be applied over others.

Meridia can configure the Client's CloudVOTE instance to optimal patch/update schedule based on Client's requirements as specified in the contract.

Q: What measures are in place to prevent upgrades from breaking Client integrations? Do you issue release notes and recommendations in advance of each upgrade (for example: guidelines on where, when, and how to perform regression testing)?

A: Given above answers about limited nature of Meridia's involvement in urgent/critical patch and service pack deployment by Microsoft Azure maintenance team, we can guarantee:

- extensive testing before patch/upgrade implementation in case the patch/service pack is in our control.

- Client will have an opportunity to test and accept the upgrade before being deployed.

Q: Have your hosting facilities been rated by the Uptime Institute or similar organization? If so, please provide the rating and date rated.

A: All CloudVOTE Microsoft Azure deployment uptime guarantees are governed by official SLA documentation found at https://azure.microsoft.com/en-us/support/legal/sla/summary/.

Q: Are third parties involved in your provisioning of data center services? If yes, please identify those third parties, services and provide websites and contact information if possible.

A: Not on Meridia's side. Microsoft manages Azure environment.

Q: Does your solution support one or more secure varieties of File Transfer Protocol (FTP)? Explain the general mechanism and standards supported.

A: Meridia uses the SFTP protocol, Secure File Transfer Protocol. The Secure File transfer Protocol ensures that data is securely transferred using a private and safe data stream. It is the standard data transmission protocol for use with the SSH2 protocol. Before establishing a connection, the SFTP server sends an encrypted fingerprint of its public host keys to ensure that the SFTP connection will be exchanging data with the correct server.

Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network.

Q: What technical documentation can you provide Clients for your solution's APIs?

A: Meridia (CloudVOTE SaaS) does not provide any public APIs.

Q: Can your Clients export data from your solution to their own cloud solutions and if so how (e.g., do you use a Docker based approach, or something else)?

A: Yes. By default, export to variety of formats is enabled:

- Excel

- Word

- CSV

Client can opt-in for SFTP transfer of a custom format (e.g. XML) if integration with Client's own third-party solution is needed.

Q: What Client PC/laptop operating systems (Windows, Macintosh, etc.) does your solution support? Differentiate by OS version if/where appropriate.

A: Minimum System Requirements are:

Microsoft Windows 7, 8, 10 (32bit + 64bit)

Microsoft Office 2010, 2013, 2016 (32bit + 64bit)

USB 1.0 or higher

250MB or more of installation space + any storage space needed for Client's local data

4GB RAM (8GB recommended)

Core i3 CPU (Core i5 recommended)

Q: What Client PC/laptop browsers (Internet Explorer, Firefox, Safari, etc.) does your solution support? Differentiate by browser version if/where appropriate.

A: IE11, Firefox 55 or higher, Edge, Chrome 55 or higher.

Q: What Client smartphone and tablet operating systems (iPhone, iPad, Droid, Android, etc.) does your solution support? Differentiate by smartphone and tablet OS version if/where appropriate.

A: Any smartphone OS with internet browser (default brand browser, Chrome mobile, Firefox mobile, etc...)

Q: What server operating system(s) (Windows, Linux, other flavors of UNIX, other) does your SaaS solution run on? Are certain solution functions limited to a certain OS? Differentiate by OS version if/where appropriate.

A: Microsoft Windows Server.

Q: What application server environment(s) (WebLogic, WebSphere, other) does your solution run in? Differentiate by application server version if/where appropriate.

A: Windows Web App Service.

Q: What web server(s) (Apache, IIS, other) does your solution run on? Differentiate by web server version if/where appropriate.

A: IIS.

Q: What database management system(s) (Oracle, SQL Server, DB2, other) does your solution run on? Differentiate by DBMS version if/where appropriate.

A: SQL.

Q: For Client-side implementations of your solution (including browser version, offline-access version if applicable, tablet and smartphone versions if applicable), what data is cached Client-side? How is such data deleted or otherwise managed at session termination? If answer differs for each solution, please provide all relevant responses.

A: Meridia applications do not store any browser/Client-side data in cache or cookies.

Q: If data is clustered, mirrored, duplicated or otherwise distributed, can the physical location of data be changed without Client's knowledge or consent? If so, if Client needs to recall, delete, or otherwise modify distributed data, can you furnish all the location(s) of all such distributed data to Client for those purposes?

A: No. Client's data will not be moved or distributed without Client's knowledge and prior approval.

VENDOR MANAGEMENT

Q: Describe all third-party vendors your organization does business with that will have access to in-scope systems and Client data.

A: Client data is accessible to the Microsoft Azure team, indirectly. All remaining vendors are shielded from customer's data and provided access on an as needed basis or to help fix any fault in the system. Meridia also tries to limit access to the data, in this scenario as well, and tries to first duplicate the issue on staging environments.

Q: Describe how your organization evaluates your third-party partners (vendors) to ensure they adequately support the availability, confidentiality and integrity required by your Clients.

A: Meridia is very selective in its hiring of third-party vendors. For software development outsourcing, Meridia requires that the vendor has industry standard certifications in place. Meridia's current software vendor is ISO9001:2008 quality management system certified and CMMI Maturity Level 2 Appraised by the Software Engineering Institute of the Carnegie Mellon University. Their employees are trained on software security standards (HIPAA) on an ongoing basis.

For infrastructure outsourcing, Meridia has selected Microsoft's Azure platform which is one of the top three cloud "Infrastructure-as-a-Service" (IaaS) and "Platform-as-a-Service" (PaaS) solutions.

For hardware vendors, Meridia outsources its proprietary hardware development to ISO9001 certified vendor.

Meridia management believes in long term vendor engagement. All our vendors are with us for more than five years eliminating risk of new vendor unpredictable performance etc.

APPENDIXES

Required Service Levels and Service Level Credits – Sample.pdf
CloudVOTE Disaster Recovery Plan Standard Response.pdf
CloudVOTE Physical Security and Information Security Standard Response.pdf
CloudVOTE Resiliency and Backup Standard Response.pdf

CONTACT INFORMATION

In case of any further questions and/or clarifications, don't hesitate to contact us at support@cloudvote.com or 610-260-6800 x117