Maimonides Information Security

Vendor Assessment Questionnaire

Revision 03.21.2024

Tesira

____

[Vendor Name]

Organization Contact Information	
Company Name	Tesira
Application Name	Biamp
Primary Contact Name and Title	Ben Klein
Primary Contact Email	bklein261@gmail.com
Primary Contact Phone	201-280-6512
Secondary Contact Name and Title	
Secondary Contact Email	
Secondary Contact Phone	
Assessment completed by	Ben Klein
Date	5-30-2025

Maimonides Sponsor and Information Security Assessor		
Maimonides Medical Center	**Department**	Simulation Lab
	Contact	Amish Aghera
	Email	aaghera@maimo.org
	Phone	(718)283-1425

Comments:

Maimonides Information Security: Informationsecurity@maimonidesmed.org 347-831-6747	**Information Security Assessor**	Dinsdale Lee
	Phone and email	(718)283-1350

Notes:

Please aim to include documents for product overview, data flow diagrams, net flow diagrams, (and a SOC 2 Type II report if your product has Cloud Service Provider dependencies).

1.1. LAWS, REGULATIONS, STANDARDS, AND GUIDANCE

Maimonides Information Security has utilized industry best practices and guidelines to assess compliance with Maimonides Policies.

Sources:

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 revision 5 – security and privacy controls for information systems
- NIST SP 800-53A revision 5 – procedures for assessing security and privacy controls
- NIST SP 800-144 revision 5 – guidelines on security and privacy practice for public cloud computing
- NIST SP 800-207 - zero trust architecture
- NIST SP 800-128 revision 5 – security-focused configuration management of information systems
- PCI Security Standards Counsel PCI DSS version 4.0
- New York State Office of Information Technology Services (ITS)/Enterprise Information Security Office (EISO) Polices and Standards
- Center for Information Security (CIS) Top-20 Critical Controls
- Health Insurance Portability and Accountability Act (HIPAA) Security Rule 45 CFR Part 160 and Subparts A and C of Part 164

1.2. PURPOSE

The Maimonides Medical Center Information Security Team is tasked with assessing all potential technology solutions and service providers for compliance with MMC policy. Technology solutions, as defined by MMC, encompass any service or solution utilizing Maimonides' on-premise data center and/or hybrid-computing environment. This includes, but is not limited to, Software-as-a-Service, Infrastructure-as-a-Service, and Platform-as-a-Service providers, in addition to any cloud-based email and document storage platforms. The goal is to ensure that established standards and regulations, which Maimonides must adhere to, are met. These standards encompass proper data protection, identity and access management, availability, and effective incident response and disclosure practices.

Maimonides Security Assessment

General Questions

Control	Response	Answer/Comments
Will this solution collect, store or otherwise process Maimonides EPHI (Electronic Protected Health Information) or PII (Personal Identifiable Information)? Please detail.	No	Tesira does not store or manage any EPHI or PII
Is there a signed Business Associate Agreement in place with MMC?	No	None Required (No PHI)
Does the platform conform to HIPAA standards?	N/A	Not Applicable
Does the platform comply to other standards or regulations? Ex. HITECH, PCI/DSS.	Yes	CE UL, and RoHS compliant.
Maimonides Information Security require a user account for testing purposes. If there are multiple roles within the application then an account for each role is required.	N/A	Tesira is configured via local software and does not utilize

Architecture and Software Isolation Disclosure

Control	Compliance	Answer/Comments
Share the architecture and underlying technologies that are used.	Yes	Tesira is an on-premises digital signal processing
Define and whiteboard their software isolation strategy Software isolation seeks to separate data and processes within the software environment itself.	Yes	It will be running on a VM in a controlled environment.
Provide timeline for advancing its infrastructure from a Public Cloud proprietary architecture (i.e. AWS) to a Containerized Applications configuration and Kubernetes	N/A	Tesira is an on-premises solution and does not utilize

Identity and Access Management

Control	Compliance	Answer/Comments
Vendor must ensure that adequate safeguards are in place for identity and access management.	Yes	Access to Tesira hardware is managed through network
Vendor must to the extent practicable, integrate with Maimonides' Directory Services for authentication and authorization. If integration with Maimonides Directory Services is unavailable at the time of implementation, the CSP must provide a timeline for integration.	N/A	Tesira does not support integration with external directory services.
Does this solution employ multi-factor authentication?	No	Tesira does not support multi-factor
Does the solution use SAML 2.0 Identity Provider (IdP) for Single Sign-On and SAML Identity Provider integration?	No	Tesira does not support SAML 2.0 or Single Sign-On
Vendor must provide Maimonides with all system access logs, activity logs and event logs within ten (10) business days of request.	Yes	Tesira systems can provide logs upon request.
Vendor must provide Maimonides with an annual compliance audit reports performed by an independent agency.	No	Please contact Biamp directly for information on compliance

Data Protection

Control	Compliance	Answer/Comments
Identify the data protection control standard it uses (e.g., HITRUST, NIST, etc.) for its data management solution and define its ability to control access to data.	N/A	Tesira does not store data; it processes audio signals in
Identify the encryption protocols and standards used to: o Encrypt data at rest o Secure data transit. o Protections for data in use	N/A	Tesira does not store data; network security is managed through standard IT practices.
The encryption keys used to secure Maimonides data will be held by Maimonides Information Security.	N/A	Tesira does not utilize encryption keys for data
Vendor must use a VPN IPSEC connection for system data exchanges, interface or otherwise, to eliminate man-in-the-middle attacks.	N/A	Tesira operates within a secured local network; VPN is
Vendor must detail the environment's use of IP access control restrictions including, but not limited to: o IP Whitelisting o Geolocation IP Fencing o Impossible Travel Alerting o Intrusion Detection Systems (IDSs) o Intrusion Prevention Systems (IPSs)	N/A	Network security measures are managed by Maimonides
Vendor must, with respect to Maimonides data, not deviate from the mutually agreed upon data protection and access controls	Yes	Tesira does not store or manage data, compliance is
Vendor must ensure that Maimonides data including EPHI, (Electronic Protected Health Information), PII (Personal	Yes	No data is shared or

Identifiable Information) or any de-identified data is not shared with, viewed, accessed by or sold to another entity.		
Vendor must have controls in place to ensure that Maimonides data resides in data centers within the continental United States.	N/A	Tesira is an on-premises solution
Vendor must permit vulnerability and penetration testing by Maimonides Medical Center or an authorized subcontractor and remediate all security vulnerabilities affecting the cloud environment at no additional cost to Maimonides. Such vulnerabilities include, but are not limited to, deprecated security protocols, unsupported operating systems and zero-day exploits.	yes	As it is installed within their network. its Security posture can be assessed by Maimonides IT as needed
Vendor must upon request, share with Maimonides the patching and maintenance schedule for all components of the cloud environment.	N/A	Tesira does not operate in a cloud environment
Vendor must demonstrate that the use of its services complies with all pertinent laws and regulations governing the handling of EPHI, PII, corporate financial data or any other Maimonides data.	yes	Tesira does not handle sensitive data
Vendor environment is protected by Anti-Virus and Anti-Malware using an enterprise class anti-virus/EDR/XDR/MDR technology.	N/A	The software is running on a maimo vm. so AV software is

Availability

Control	Compliance	Answer/Comments
Vendor must provide uptime availability SLAs including any exceptions to those guarantees.	N/A	Tesira is on-premises so
Vendor must for any Cloud Service Subcontractors it uses, identify the contract provisions and procedures regarding data availability, data backup and recovery, and disaster recovery such that Maimonides IT personnel may ensure that such provisions and procedures meet Maimonides's continuity and contingency planning requirements.	N/A	Tesira does not utilize cloud services
Vendor must ensure that during an intermediate or prolonged disruption or a serious disaster its critical operations (and those of its Cloud Services Subcontractors) can be immediately resumed, and that all operations can be reinstituted in a timely and organized manner.	Yes	Tesira's on-premises nature allows for direct control over disaster recovery procedures
Vendor must provide downtime workflow or procedures to ensure business continuity in the event of an Internet outage or other disruption.	Yes	Tesira operates independently of internet connectivity
Share all data backup and recovery methodologies and detail all disaster recovery strategy.	N/A	Tesira does not store
Vendor to provide architecture diagram and provide details of Internet Connectivity and ISP redundancy.	N/A	ISP Connectivity not needed
Vendor maintains immutable data backups of customer data.	N/A	No Customer data handled

Incident Response and Disclosure

Control	Compliance	Answer/Comments
Vendor must ensure that any Cloud Services Subcontractors it uses will clearly identify the provisions and procedures for incident response in the arrangement between such Cloud Services Subcontractor and the CSP.	N/A	Tesira is an on-premises solution and does not rely on third-party cloud service
Vendor must in the event of a Breach or Security Incident (each as defined at 45 C.F.R. Part 164) or any other unauthorized acquisition of Maimonides EPHI or PII, ensure that Maimonides can respond to incidents in a coordinated	N/A	Tesira does not collect or store EPHI or PII, and does not operate as a cloud-based

and transparent fashion with the CSP and, if applicable, the Cloud Services Subcontractor.		
Vendors must notify Maimonides IT team as soon as practicable (but no later than 10 business days from the discovery date) regarding a Breach or Security Incident (each as defined at 45 C.F.R. Part 164) or any other unauthorized acquisition of Maimonides EPHI or PII.	Yes	In the event of a system vulnerability or exploit affecting Tesira devices, Biamp typically communicates

Provider (Vendor) Infrastructure Assessment Section

Control	Compliance	Answer/Comments
Who is responsible for cybersecurity within the organization? Is there chief information security officer (CISO) or equivalent?	Yes	Contact Biamp for an official name/title.
Do you continuously assess and remediate your organization's cyber vulnerabilities? If so, please describe methodology	Yes	Biamp releases regular firmware updates to address
Is there a process for reviewing and updating security controls based on changes in the threat landscape?	Yes	Biamp monitors evolving
Are developers trained on secure development best practices such as using a memory safe programming language?	Yes	Biamp adheres to secure
Are you SOC 2 Type 2 compliant? Please share the latest report.	N/A	No sensitive data is handled
Vendor is ISO/IEC 27001 certified.	N/A	No sensitive data is handled
Are cybersecurity incidents reported? If so, please describe methodology	Yes	via firmware advisory
Have you ever experienced a significant cybersecurity incident? Please define and describe it.	No	None publicly reported as o
When was the last time you had a cybersecurity assessment performed by a third-party organization? What were the results of that?	Yes	Verify with Biamp
How frequently does a third party perform a vulnerability assessment or penetration test?	Yes	security verification is internal
Do you have automated tools that continuously monitor to ensure malicious software is not deployed	Yes	Tesira runs on dedicated
Does your organization have a 24x7 SOC?	No	Not needed as no sensitive
Do you enforce multifactor authentication before your employees and/or third-party partners are granted access to the backend resources/infrastructure?	Yes	there are no exposed backend resources
Do you enforce password complexity and what is the minimum password length?	Yes	Tesira system access can be
Do you require password resets? Ex. 120 or 180 days	No	No user passwords or
Do you enforce an EOL (End of Life) policy for all servers and endpoints? Windows and/or Linux	Yes	Biamp publishes product
Vendor shall review all patches, updates, and upgrades of operating systems, middleware, or applications to all relevant components of the Services after they have been released by the manufacturer. Vendor shall manage the patching process expeditious to assure that critical patches are applied in a timely manner consistent with the leading practices and generally within 30 days of release.	Yes	Biamp regularly publishes firmware updates and encourages users to stay current to maintain security and stability.
Do you monitor privileged accounts? If so, please describe methodology	N/A	no privileged accounts
Do you have processes in place to prevent the exfiltration of sensitive data, particularly sensitive customer data like ours? If so, please describe methodology	Yes	Tesira systems do not store sensitive data, and there is no

Infrastructure of the Data Center: Vendor and/or its sub-processor(s) shall monitor the infrastructure in order to identify any security vulnerabilities.	Yes	We will update firmware regularly
Vendor utilizes secure network architecture principles including network segmentation, access controls and role-based least privilege for hosts, services and users.	Yes	The Network architecture is provided by Maimonides
Vendor requires the use of a multi factor authentication for remote access to vendor's network.	Yes	I log in using the Maimonides
Vendor has disabled Remote Desktop Protocol (RDP) on all devices within their network.	N/A	This is managed by
Vendor has enabled a leading email security solution to scan all incoming emails, attachments and URL's for malware or malicious links.	N/A	Tesira does not use email

Mobile Component/Application *(if applicable)*

Control	Compliance	Answer/Comments
Is there a mobile application for this solution?	No	Tesira has no Mobile
Which platform/s does this mobile application run on? Android/IOS or both	N/A	There is no Mobile Application
Will this mobile application be installed on Maimonides sponsored devices, personal mobile devices or both?	N/A	There is no Mobile Application
Has the mobile application undergone any third-party / OWASP (Open Worldwide Application Security Project) pen-testing?	N/A	No Mobile Application
(Android) What kind of permissions does the application require and what is optional?	N/A	No Mobile Application
Does your app have different user roles? How many different user roles do your app need to support? Can you provide an overview of each role and list the features each role can access?	N/A	No Mobile Application
(iOS) Does your app use mobile sensors? Do some features require the camera, microphone, GPS (location-based services), compass or accelerometer? What does your app do with sensor data?	N/A	No Mobile Application

Document Request *(if applicable)*

Documents Requested	Compliance	Answer/Comments
Dataflow Diagram	Yes	Tesira system dataflow is
Network Diagram	Yes	Maimonides IT can provide
Third party risk assessment	Yes	Maimonides can Assess
SOC 2 Type II Report	N/A	Tesira is On-Premesis
Bridge Letter (This may be needed if the SOC 2 Type II report has any gaps)	N/A	Tesira is On-Premesis
Hi-trust Certification	N/A	No PHI
Additional Documentation	Yes	Available on the Biamp

Vendor comments:

Biamp Tesira software is a slim client for configuration of the Tesira Hardware. It does not manage PHI or communicate outside of the closed network. The software will be running on a Maimonides provided VM with all components located within their secure network.

By signing below, I represent and warrant that I have the knowledge and authority to answer this Security Assessment on behalf of vendor, and that all answers provided to this assessment are complete and accurate. I will immediately notify Maimonides Medical Center if any of the answers change or are discovered to be inaccurate.

Benjamin Klein

_______________________________(05/31/2025)

[Signature] [Date]

Software Developer

____

[Name & Title]