MERIDIAN
CONCEPT TO COMPLETION

FLEX
TECHNOLOGY GROUP

PERSONNEL MANAGEMENT SOLUTION

SOFTWARE SECURITY & COMPLIANCE REVIEW

ACCESS CONTROL

What is the password policy used for your admin accounts accessing your platform (infrastructure or applicative)?	Passwords must be rotated every 30 days and must conform to minimum password strength requirements. Accounts with more than 3 password failures are locked for 1 hour. We employ SSO tokens where practical.
Are passwords encrypted at rest and when exchanged? Do you have a “forgotten password request” mechanism?	Passwords are encrypted and salted, an administrator may reset the password for users.
Hierarchy system rights accessibility (tier level)	The MzeroManage Platform supports tiered rights for individual users and groups.
Can we use our WebSSO solution (SAMLv2, OAuthv2) with your Saas application?	Not at this time.
Does the application support token / certificate-based access (in case of API access)?	Not at this time.

APPLICATION SECURITY CODING AND TESTING

Please describe your practices in secure coding (developer security training, dev environments, code reviews, SDLC, bug tracking, etc.).	We employ an internal ticket management with the JIRA system, we also employ peer-review techniques for code and enforce good development practices internally. We also adopt latest security standards as fast as possible.
Describe your TLS security ratings	For our hosted solution at https://personnel.meridiankiosks.com this results in an A rating. We have a B rating for http://www.mzeronet.com/ on account of having to support TLS1.1 for some legacy clients. *Rating based on test from ssllabs.com
Do you perform vulnerability scans on the platform? If yes, what is the date and outcome of last test?	We are scanned by Clover security periodically as part of our PCI assessment maintenance.
Do you perform penetration tests / code audits on the platform? If yes, what is the date and outcome of last test?	We had some of our clients perform independent audits by security contractors but I don't have specific details on who and where these tests were conducted. For example, we have had our software pass tests for Federal government agencies (NOAA).
Do you have a bug bounty program?	No

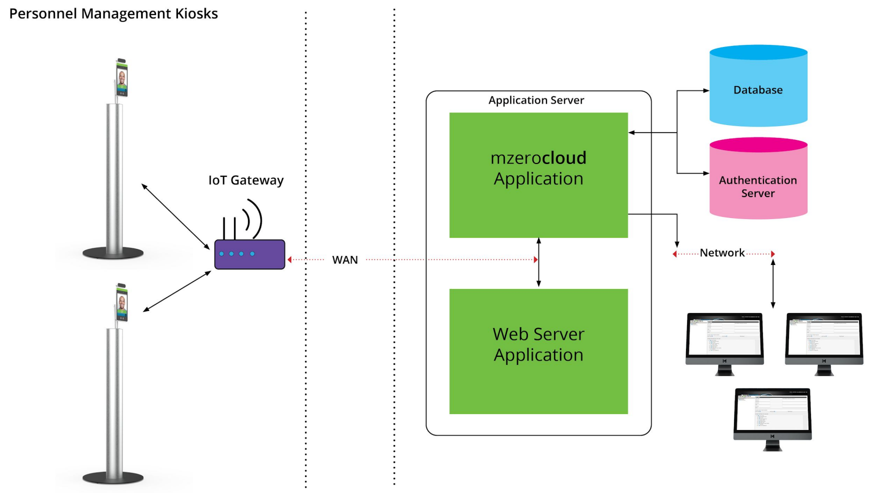
AVAILABILITY, BUSINESS CONTINUITY & DISASTER RECOVERY

What is your application uptime commitment?	Our SLO is 98.9%
Do you have a disaster recovery plan?	Yes we have an internal disaster recovery plan/process. We maintain 5 day rolling backups of our server-side infrastructure, a complete restore would take between 1-2 business days. Enhanced backup and emergency response disaster recovery is available pursuant to an agreement.
How scalable is your platform/service? How do you manage capacity planning?	Our VPDC environment can add additional capacity both horizontally and vertically to meet any demand.

DATA ACCESS & SECURITY

How can we access to the platform? Please describe security of these flows/interfaces (HTTPS, API, (s)FTP, etc.)	HTTPS access there is an administrative portal.
Can this cloud solution interface with Google G-Suite : Gmail, Docs, Drive, Agenda, etc.?	It does not
Reversibility: Please describe the ability for client to export data from the platform with a standard, exportable and exploitable format?	You may pull reports generated out of the system via CSV we also have an API where an authenticated user may download historical reports (archive service).
Please describe the ability for client to delete our data from the platform?	You may arbitrarily delete all kiosk activity as needed, we can also reset your client database at your request by doing so to help@mzero.com.
Please describe the security of the wireless keyboard that comes with the device	We have introduced a wireless keyboard to replace an exposed USB port, for security. The USB port is on a frequency tied to the brand and serial number of the keyboard for which it is connected to. The communication is not encrypted. An encrypted wireless keyboard can be used with this device if purchased elsewhere.

ENVIRONMENT ACCESS & SECURITY

High Level Architecture	 Personnel Management Kiosks IoT Gateway WAN Application Server mzerocloud Application Web Server Application Database Authentication Server Network

ENVIRONMENT ACCESS & SECURITY CONT.

How is the connection between the IoT Gateway and MzeroManage encrypted?	The connection between MzeroMange IoT Gateway and MzeroManage is TLS1.3 encrypted strong ciphers and is both HTTPS and Websockets connectivity.
What are the categories of provider's employees or contractors with access to customer's data? (e.g. Developer, Administrator, Database Analyst, Helpdesk.)	If you choose the Meridian hosted solution, only Meridian Sr. Software engineers have access to your server or data through a site-to-site VPN connection to the data center from our central office for the purpose of maintenance and updates to the software technology. We will not access your data.
How do you enforce security of these personnel accesses to the platform? (HR, training, access management, review, etc.)	We have a small team of members who are controlled by a central federated identity management solution, those with access to the system have been trained on the operation of the solution and the protection of the data.
How do you enforce "data at rest" security (location, encryption, access control)?	The VPDC disk volumes are encrypted, additional encryption on fields are also possible where mandated, pursuant to an agreement to provide such enhanced encryption.
Do you use web application firewalls or filtering reverse proxy or similar?	If you are looking to deploy web application firewalls we offer this as an optional upgrade service through a Juniper-branded firewall device. We do employ reverse proxy solution through Apache and NGNX as well as firewall restrictions in the OS and at the ACL access control at the gateway device.

IDENTITY & ACCESS MANAGEMENT

What are the processes and tools for client's users creation / modification / deletion?	MzeroManage software has an internal user management solution for device administrators.
Is there a possibility for a connector with our IAM solution (IBM Tivoli) so that we can manage the users in our standard interface?	Not at this time.

LOGGING, ALERTING & INCIDENTS MANAGEMENT

What security monitoring do you do in the platform? What logs exist on the platform (events, type of informations)?	The kiosk software tracks all logins and audit trails of changes using Integrity Control.

INTELLECTUAL PROPERTY RIGHTS

Provide a full disclosure of the IP ownership of the technology being provided (i.e., is it owned by your company, licensed, open source, etc.).	Meridian maintains full IP ownership of Meridian developed software. We have appropriate reseller agreements in place for all of our third party software solutions and add ons.

HOSTING & INFRASTRUCTURE

Who is your Hosting provider?	Centurylink
Where is your hosting location?	Virginia
Who has the ownership and responsibility for security maintenance of Infrastructure layers? (OS, Databases, networks, etc.)?	Meridian - Software Team
What is the level of mutualization of infrastructure (infrastructure servers/networks/database/appli shared or not)? If applicable: how is customer data are segregated from other customers?	Our Optional MzeroManage product is Meridian's hosted environment is multi-tenant, we also offer hosted services on a dedicated server if you require for an additional cost for the virtualization environment. We also have an on-premises solution available.
Operating system, data storage: please give us an overview of technologies used.	We typically use RHEL 7 (Soon RHEL 8) or UBUNTU 18.04 for our cloud environment.
Please describe how data is backed up and backups security.	We have a secondary backup location nightly in a different data center Washington state, the backup is transferred over a VLAN site-to-site.
Internet access: what is the number of presence points, bandwidth, anti DDOS mechanism, use of a content delivery network?	Our hosted services utilize firewalls IP access restrictions, we have additional firewall upgrades available which feature IPS and a dedicated Juniper Firewall Appliance for those with a dedicated hosted instance for an added cost.
What are the certifications of hosting provider (ISO 27001, SSAE16, Tier 3, 4, ANSSI...)?	SOC1, SOC2
Please, describe your physical security and safety.	We are SOC1 & 2 certified which encompasses the facility's physical security and safety

POLICY, CERTIFICATION & ASSURANCE

Do you have security certifications (ISO 27001, SSAE16, Tier 3, 4, ANSSI...)?	No certifications.
Have you been evaluated by a cybersecurity rating firms (e.g. Ecovadis, Cyence, BitSight, SecurityScorecard, Cybernance, RiskRecon...)?	We've been evaluated for specific solutions by NCI Inc., CoalFire, InfoSec Integrators, and Clover Security primarily for Payment related solutions as well as routine scans and stress tests. We've also been independently reviewed by several of our clients in the past, some of which include NCR Corporation, BMW, MetLife, and Husqvarna.
Do you have a Cyber Insurance?	Yes

FLEX
TECHNOLOGY GROUP

For more information,
please contact your
FTG representative.

Flex Technology Group
Corporate Headquarters
2845 N Omaha, Mesa, AZ 85215

www.flextg.com
ph: 888-353-9774
email: info@flextg.com