MarshallGIS

IT Policy

7/31/2020

2915 N. Cole Rd.

Boise, ID 83704

Phone: (208) 514-0411

LiGOSales@marshallgis.com

www.marshallGIS.com

Table of Contents

Section 1 - Security

1.1 - Data Center

- MarshallGIS' Data Center is secured behind double locked doors, accessible via multifactor authentication with limited access to only a few, vetted, essential, "need to know" MarshallGIS long-term employees, and protected by 24/7 monitoring, security cameras and by a dry chemical fire suppression system. Physical access can only be gained with logged multifactor authentication.
- The isolated LiGO® network is protected by Cisco zone base firewall and SNORT intrusion protection systems with all access being logged and recorded.
- LiGO® systems can only be accessed by the senior systems engineer and senior development engineer. Administration applications and tools can only be accessed from within onsite networks.

1.2 - Weakest Link Methodology

- MarshallGIS uses "weakest-link" methodology: Conventional defense in-depth methodologies fail with weak barriers and questionable human access. MarshallGIS' barriers are rock solid with systems access limited to only a few MarshallGIS employees all of whom are high skilled, vetted and experienced engineers. New IT staff are subjected to background checks, IT apprenticeship and testing. Current IT staff have ongoing education requirements and system training. Along with this methodology, MarshallGIS follow vendor recommendations, industry standards and accepted best practices with a common-sense approach.
- Systems on the LiGO® network can only be accessed via RDS or remote console from desktops within MarshallGIS' internal trusted network.
- All end users' primary work systems on MarshallGIS' trusted network have Trend Micro Security Suite Client which prevents viruses, malware, spyware, grayware, ransomware and checks user's activity. All employees are required to sign acknowledgement of the employee handbook which include, but not limited to, the following:
    - Using separate personal and business computers, mobile devices and accounts
    - Not connecting personal or untrusted storage devices or hardware to corporate computers, mobile devices or networks
    - Not removing MarshallGIS storage devices from the MarshallGIS network or building
    - Only using approved software
    - Not giving out personal or business information
    - How to create and use strong passwords
    - How to handle email attachments and web links
- In addition, Security Policies and Procedures are reviewed at staff meetings and mandatory annual training.

1.3 - Application, Operating Systems and Hardware Monitoring

Continuous monitoring is established via PRTG, Dell OME and Veeam One monitoring software using Netflow services, Simple Network Management Protocol (SNMP), Windows Management Instrumentation (WMI), networks and logs. System vulnerability is managed with these monitoring systems and their logs are reviewed weekly, while vulnerability testing is completed quarterly. Any unusual activity is immediately investigated.

1.4 - Data Containment

Every effort is made to keep files and data within the confines of MarshallGIS' networks. Files are not stored in public cloud storage, Mobile User VPNs are not used to access any MarshallGIS network, and work is done only on MarshallGIS owned devices.

Section 2 - System Maintenance

2.1 - Windows of Maintenance

MarshallGIS has two windows of maintenance that occur each month:

- Microsoft Windows updates are installed the evening on Saturday, following the first Tuesday of each month
- LiGO® updates occur the evening on the first Sunday of each month

The days and times of these updates are chosen in the hope that these updates do not cause system down time during normal business or working hours – as the potentiality of system and access interruptions during these update periods are existent. The update periods also allow MarshallGIS to run tests and ensure that the updates are not causing any failures or problems elsewhere within the LiGO® system before release.

Section 3 - Incident Response Process

NOTE* MarshallGIS has never had a security incident

Customers will access tech support via a 24/7/365 web portal to report incidents, failures, concerns, and complaints.

3.1 - Response Process

1. **Preparation:** We train our employees and IT staff to handle potential incidents should they arise
2. **Identification:** Incidents are posted in MarshallGIS' portal/CRM. Incidents are analyzed, classified, and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach. Identified incidents are reviewed, monitored, and investigated by our incident response team.
3. **Notifications:** MarshallGIS incident response process specifies notification to all customers concurrent with the process. Customers will be notified by email and status of the incident will be posted on the MarshallGIS web portal.

4. **Containment:** We limit damage from the incident and isolate the affected systems to prevent further damage
5. **Eradication:** We find the incident's cause and remove affected systems from the production environment
6. **Recovery:** We allow affected systems back into the production environment and ensure no threat remains.
7. **Lessons Learned:** We document the incident and analyze how it happened so staff can learn from it and improve future response efforts. Critical incidents are investigated and addressed, lessons learned are documented and analyzed, and incident response plans and recovery procedures are updated based on the lessons learned.

Section 4 - Data Stewardship

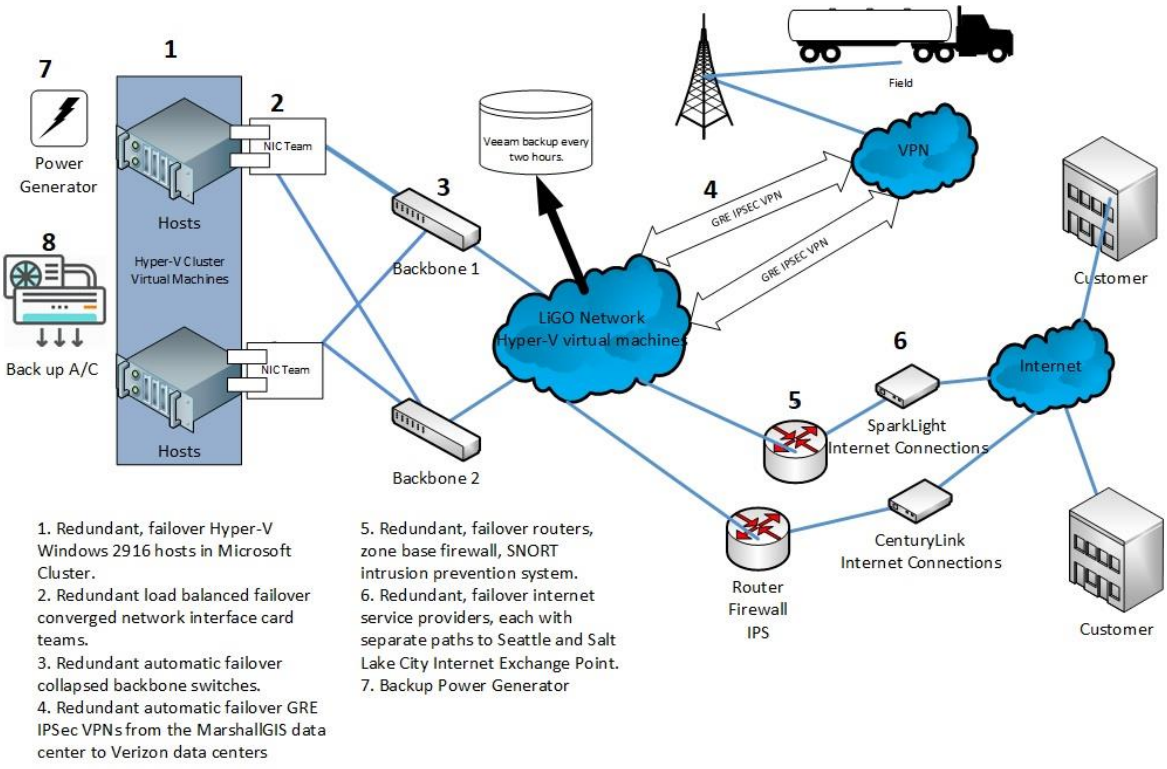
- Data Ownership
    - Customer owns its data and can download it via reports. Data can also be delivered to customer via SQL Server backup database file (may be charge associated due to work preparing file)
- Data Sharing
    - MarshallGIS does not provide, sell, or share any data to any third parties without prior written approval.
- Data Retention
    - Data is kept for a maximum of three years unless otherwise agreed upon
- Data Deletion at Contract Termination
    - The application and all data pertained are deleted after termination of contract unless customer requests in writing otherwise
    - Storage media is certified destroyed when disposed of
- Data Transfer (In Transit Encryption)
    - All cellular private network device communications occur via encrypted redundant AES 256 IPSEC tunnels to MarshallGIS' secure servers and are inaccessible from the Internet
    - Customers may access their application through SSL (TLS) signed with CA certificates
    - Customers may limit access to their application from specific networks and use SAML, ADFS, or Okta for secure access. MarshallGIS only use secure versions of protocols. Web and code signing certificates and passcodes are stored in secured storage applications and destroyed after expiration
- Data Storage (At Rest Encryption)

- Any customer's Personally Identifiable Information (PII), Electronic Health Information (EHI), Federal Tax Information (FTI), or Primary Account Numbers (PAN) stored in LiGO® or MarshallGIS associated servers, at rest, are encrypted using AES 256 or better encryption

Section 5 - Business Continuity Policy

5.1 - Resiliency

The IT staff ensures every component of the LiGO® system is redundant with failover to prevent outages and to survive disasters. The LiGO® network has end-to-end fault tolerance and redundancy. All component including VPN Tunnels, ISPs, modems, routers, switches, network interface cards and servers have automatic failover. Automatic failover is tested and proven routinely.



MarshallGIS specific Disaster Recovery and Business Continuity Procedures are kept confidential for security reasons.

5.2 - Back Up Policy

All data and servers are fully backed up every three hours. Backup disks are rotated to a bank vault offsite weekly. Backed up data is available a minimum of 30 days for full system recovery. In addition, a January full backup is completed each year and stored indefinitely. Customers can coordinate and archive data retention within their specific LiGO® application.

MarshallGIS uses Veeam Backup and Replication: https://www.veeam.com/vm-backup-recovery-replication-software.html with a full hypervisor virtualized environment running backups every three hours. This allows instant database server recovery to any Hyper-V host or the Azure cloud service.

5.3 - Plan, Review and Update

The IT department reviews this policy as part of its quarterly system checks and procedures and makes changes and updates as necessary.

5.4 - Posting

The IT department creates, updates and posts emergency actions in the network room, bank vault and in the IT file cabinet.

5.5 - Notification

The EAT (Emergency Action Team) will be notified of an outage via one of several monitoring systems which text and email individuals on the EAT. Every component of the LiGO® system is monitored. Any employee will contact the EAT if they identify an outage or critical situation as part of their job duties. Specifically, the help desk staff may identify an outage or situation when receiving a customer call, at which time they will contact the EAT.

5.6 - Audit Logging

The LiGO® systems logs user actions. MarshallGIS keeps maintenance logs including firewall, IPS, router syslogs, Netflows, SNMP, Windows application, security, and system event logs. MarshallGIS stores logs up to a year depending on log type.

Revision History

Date	Author	Changes Made
1/1/2020	Ken	Rewrite of this policy to meet specific requirements
3/3/2020	Shawn	Formatting to MarshallGIS standard
7/31/2020	Ken	Revised Incident Response Section to better meet requirements Modified revision history table