Security Measures

PODIO.XYZ INC (DBA Spokn) uses commercially reasonable efforts to implement and maintain the security measures listed below. PODIO.XYZ INC may update or modify these Security Measures from time to time provided that the updates and modifications will not result in any material degradation of the overall security of PODIO.XYZ INC's Services.

Infrastructure/Servers

- PODIO.XYZ uses Google cloud platform to host all machines, databases and application programming interfaces.
- All infrastructure is hosted on Google Cloud servers inside the United States.
- One Security Group is allowed to access PODIO.XYZ's infrastructure.
- Our infrastructure contains two separate virtual private clouds ("VPC"s): one for Production and one for Staging.
- VPCs are only accessible from a single machine that is exposed to the internet and accessible through tunneled secure shell ("SSH").
- Two SSH keys are required to access any machines within the infrastructure.
- Multi-Factor Authentication is used on all the systems inside GCP.
- All SSH keys are RSA 2048-bit length.
- Inbound traffic for PODIO.XYZ servers is managed by Google Load Balancer, which includes heavy intrusion detection and prevention measures.
- PODIO.XYZ servers are protected from denial of service, it will be directly blocked by firewall.
- The Main Production cluster is using Google Kubernetes to manage the workloads and scale up/down when needed.
- All inbound communication is done over Transport Layer Security ("TLS"). TLS certificates are managed by Google.

Database Environment

PODIO.XYZ INC's database environment has the following database clusters

  - o Structured Query Language ("SQL") database cluster
  - o NoSQL database cluster
  - o Time Series database cluster

- Every cluster has two separate environments (Staging and Production)
- All databases' saved data is encrypted at rest

- Communication between databases and application services is done within the VPC
- Only authorized service has a firewall connection to the databases
- Databases are located inside the US
- A daily back-up for user data is saved on Google Buckets.

Access Management

From the Customer's perspective, access to PODIO.XYZ will be granted through creating a profile. We permit this action through:

- Username and password
    - Passwords must be at least 6 characters.
    - Passwords are SHA2 hashed.
    - App level manage to access using OAuth standard afterwards (access token and refresh token)
- SAML support with Google as IdP
    - User Identity will be collected for Enterprise users over secured SSO standard.
    - Only permitted data from IdP is stored to user profile
    - Access token will be assigned to this user and will be refreshed every defined time slot

Incident Management

1. All systems we have are monitored using a platform called Stackdriver from Google
2. Monitors includes:
    a. System Health Check <> Back-end Latency
    b. System Health Check <> CPU Utilization for K8s
    c. System Health Check <> CPU Utilization for VMs
    d. System Health Check <> Error logs rate is more than 50%
    e. System Health Check <> Hits are huge [6000 rpm]
    f. System Health Check <> K8s Pods Stability <> Restart count
    g. System Health Check <> SQL CPU / Read is high
    h. System Health Check <> Systems availability
3. Notification Policy for all monitors:
    a. SMS for Production Engineers to check the problem
    b. Periodical notification over Slack channel till the incident get solved

4. Postmortem and Incident report will be communicated to all our Enterprise customers and users.